Applying a Distinguished Framework to Ensure Privacy-by-Design and Composability in a Regulated Tokenized Multi-Asset Network

Rodrigo Gonçalves Bueno[*], André Luiz de Souza Carneiro[†], João Paulo Aragão Pereira[‡]

Abstract

The increasing adoption of tokenized assets, Decentralized Finance (DeFi) applications, and the exploration of Central Bank Digital Currencies (CBDCs) necessitate sophisticated security architectures for Regulated Tokenized Multi-asset Networks (RTMNs). This paper addresses the complex interplay between privacy, and composability within these emerging decentralized financial ecosystems. It is argued that conventional security paradigms, predominantly reliant on perimeter defenses, are insufficient for the distributed and interconnected nature of DeFi infrastructures. While Zero Trust models offer relevant principles, their direct application within regulated, high-performance financial networks, particularly those involving CBDCs or complex DeFi protocols, presents significant challenges regarding compliance and efficiency. This paper introduces a novel framework meticulously designed to support diverse RTMN use cases, including retail/wholesale CBDC, tokenized deposit, stablecoin and multi-asset platforms operating within a DeFi context. A foundational element of this framework is the implementation of cryptographically enforced information compartmentalization. This ensures that each architectural component operates with the minimum necessary information required for its specific function, inherently embedding privacy-by-design and preventing unauthorized access to comprehensive network or transactional data. The proposed framework is architected to guarantee critical properties essential for robust distributed and decentralized systems: (1) Atomicity of transactions; (2) Composability and Programmability; (3) Settlement Finality, providing transaction immutability; (4) Enhanced Privacy and Security, leveraging cryptographic techniques; (5) Support for Distribution and Decentralization; (6) Performance, addressing throughput and latency demands; and (7) Continuous monitoring and auditing, enabling regulatory oversight without compromising user data. It is provided a detailed analysis of the framework's application across distinct RTMN implementations, identifying specific technical challenges and opportunities within the context of tokenized systems. Furthermore, the paper presents a qualitative and functional evaluation of the framework's characteristics applied to the use case of tokenizing Federal Government Securities in an RTMN, such as Drex. Fundamentally, the inherent trade-offs between cryptographic privacy guarantees, compartmentalization, and programmability are examined, exploring optimization strategies relevant to demanding DeFi and institutional applications, such as decentralized trade finance and tokenized debt instruments.

Keywords: *DeFi, CBDC, Tokenized Multi-assets, Privacy, Composability, Compartmentalization*

[*] Chief Technology Officer at BBChain: bueno@bbchain.com.br

[†] Chief Executive Officer at BBChain: carneiro@bbchain.com.br

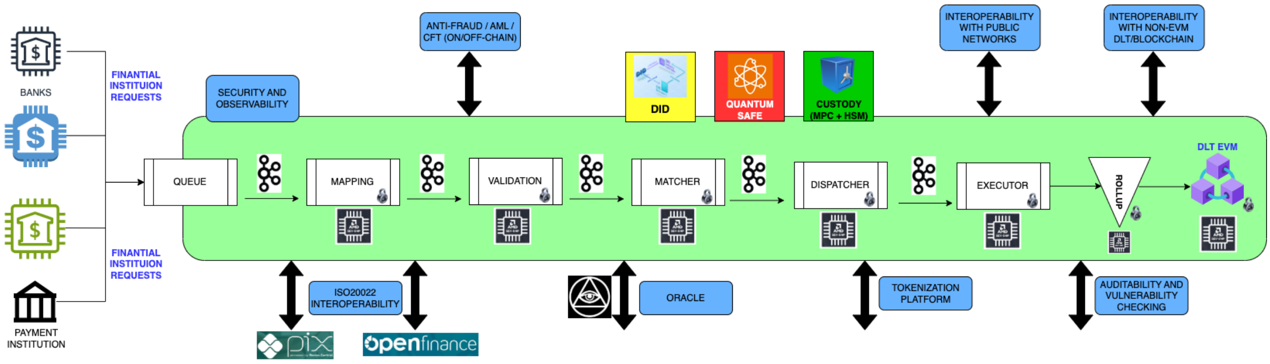
[‡] PhD, and Postdoc candidate AI/ML and DeFi researcher at POLI/USP, Expert of Innovation in Financial Services: raijoma@alumni.usp.br

1 Introduction

The proliferation of tokenized assets, the expansion of Decentralized Finance (DeFi), and the global exploration of Central Bank Digital Currencies (CBDCs) [10] signal a fundamental transformation within the financial landscape. This evolution necessitates the development of robust and sophisticated security architectures capable of managing the unique challenges posed by Regulated Tokenized Multi-Asset Networks (RTMNs). As highlighted, conventional security paradigms, often centered on perimeter defenses, prove inadequate for the inherently distributed, interconnected, and often permissionless nature of these emerging DeFi infrastructures.

Zero Trust [61] operates on the core principle of "never trust, always verify". However, while offer valuable guidance, their direct transposition to regulated, high-performance financial networks particularly those integrating CBDCs or complex DeFi protocols faces significant hurdles concerning regulatory compliance, transactional privacy, and operational efficiency, demanding more specialized solutions. In this way, the high-level framework in Figure 1 should be the ideal architecture of the Digital Public Infrastructure (DPI) [47], and it is designed by the concept of Finternet [12], which integrates advanced technology to cover some essential concepts for a financial ecosystem that uses CBDC. Asynchronous messaging follows the flow of 1) Mapping; 2) Validation; 3) Matcher; 4) Dispatcher; 5) Execution and 6) Proof of Transactions that optionally could benefit from a rollup (batch of transactions)/ZK-rollup (zero knowledge) [33], until it is persisted in a blockchain/DLT (Distributed Ledger Technology) or a database. Note that the secure environment could be running on confidential computing nodes [35], in addition to incorporating on- and off-chain anti-money laundering (AML), anti-fraud, and CFT (countering the financing of terrorism) solutions, beyond embedded security and observability modules.

Figure 1: *Zero Trust Regulated Tokenized Multi-Asset Network (RTMN).*


BANKS
FINANTIAL INSTITUION REQUESTS
FINANTIAL INSTITUION REQUESTS
PAYMENT INSTITUTION
SECURITY AND OBSERVABILITY
ANTI-FRAUD / AML / CFT (ON/OFF-CHAIN)
DID
QUANTUM SAFE
CUSTODY (MPC + HSM)
INTEROPERABILITY WITH PUBLIC NETWORKS
INTEROPERABILITY WITH NON-EVM DLT/BLOCKCHAIN
QUEUE
MAPPING
VALIDATION
MATCHER
DISPATCHER
EXECUTOR
ROLLUP
DLT EVM
ISO20022 INTEROPERABILITY
pix
openfinance
ORACLE
TOKENIZATION PLATFORM
AUDITABILITY AND VULNERABILITY CHECKING

Based on this exemplary security demand, the proposed framework (Ptah) is fully modularized, distributed and has as its main pillars the security and privacy inherent to its design. It is complemented by asynchronous messages to meet the performance required by some use cases, in addition to the compartmentalization of requests with processing by tokenized assets. It is possible to create integration plugins with interoperability tools already on the market that support coordination by a 2PC (Two-Phase Commit) protocol, to make viable the interoperability between different unified ledgers, and even public networks and platforms that use the ISO20022 [50] standard. Another essential component of the platform is the oracle service [25]; its purpose is to mediate communication between smart contracts and the Legacy Environment of a financial institution.

Addressing these intricate requirements, the proposed novel framework offers a tailored approach specifically designed for the complexities of RTMNs. Its foundation rests upon cryptographically enforced information compartmentalization, a principle ensuring that network components access only the minimum data necessary for their designated functions. This inherently embeds privacy-by-design and critically restricts opportunities for unauthorized data aggregation or access. Thus, it is possible to solve the intrinsic problems of asymmetries of most financial ecosystems: A) Financial market (Payment institution x Commercial Bank); B) Information (Privacy, not everyone can know everything); C) SLA (Service Level Agreement for different types of products); D) In addition to interoperability between the traditional financial market and tokenization and settlement platforms such as Drex [17].

The framework is architected to deliver a suite of essential properties vital for the integrity and functionality of modern financial systems: **transactional atomicity**, ensuring indivisible execution; **composability and programmability** for sophisticated financial logic; guaranteed **settlement finality**; enhanced **privacy and security** through advanced cryptographic methods; inherent support for **distribution and decentralization**;

enough **performance** to meet throughput demands; and capabilities for continuous, privacy-preserving **monitoring and auditing** crucial for regulatory oversight. On top of all this, Ptah could be composed of other advanced modules such as Decentralized Digital Identity, custody of private keys based on MPC (Multi-Party Computation) [34] and HSM (Hardware Security Module) [30], quantum-safe [38] in digital signatures or quantum-secure [57], anti-fraud, AML/CFT, among others.

The practical applicability and feasibility of this framework extend beyond theoretical constructs, offering a viable architectural foundation for prominent, real-world initiatives currently underway. Brazilian Central Bank's Drex platform, a pilot project exploring the use cases for a wholesale CBDC alongside tokenized deposits and multi-assets within a regulated environment, represents an ideal candidate for its implementation. Drex's multi-asset nature and its need to balance innovation with stringent regulatory requirements align directly with the framework's core strengths. Implementing this framework within Drex could provide the necessary guarantees for privacy between participants, composability, secure atomic settlement across different tokenized assets (CBDC and deposits), enough throughput for anticipated transaction volumes, and the auditable, compartmentalized data access required by the central bank and regulators, thereby addressing key challenges identified in the Drex pilot's design (phases 1 and 2).

Furthermore, the framework's adaptability makes it highly suitable for international collaborative projects spearheaded by the Bank for International Settlements (BIS) [9], such as Project Agorá [13] and mBridge [15]. Project Agorá, focusing on the integration of tokenized commercial bank money and wholesale CBDC on unified platforms, would benefit significantly from the framework's robust support for multi-asset operations, composability, and cryptographically enforced privacy, essential for complex interbank transactions. Similarly, Project mBridge, which tackles the challenges of cross-border payments using CBDCs, requires solutions that ensure interoperability, settlement finality, performance, and privacy across diverse regulatory and technical landscapes. The proposed framework, with its emphasis on secure and privacy-preserving operations alongside auditable compliance mechanisms, provides a compelling architectural blueprint to underpin the security and functional requirements of these ambitious international financial infrastructure projects.

1.1 Objectives and Motivation

The objective of this study is to demonstrate that it is possible to apply an asynchronous messaging framework to guarantee privacy and composability in a distributed regulated environment such as CBDC and multi-asset platforms, for example, Drex in Brazil [17]. The idea is to have a cryptographic journey where each piece of the architecture sees only what is necessary to perform its work, without allowing for completeness of information, ensuring privacy-by-design. And the main driver of this study is related to the growth of studies related to CBDC, stablecoins, and tokenized assets, with more than 110 countries at least researching [27] [60].

1.2 Expected Contributions

The main contribution of this work is to demonstrate the feasibility of implementing a modular framework to maintain privacy in permissioned CBDC environments, whether wholesale or retail, and with tokenized deposits as well as tokenized multi-assets, without compromising performance. The proposed framework could be applied to the Brazilian Drex platform and in other projects such as Agorá [13] or mBridge [15] from the BIS (Bank for International Settlements) [8], or Ensemble [40] project from HKMA (Hong Kong Monetary Authority), to maintain the security of the national and global financial ecosystem.

1.3 Document Structure

The document is structured into a series of chapters that collectively lay the groundwork, dissect methodologies, and culminate in a synthesis of findings and forward-looking insights. Session 1 outlines the demands and objectives of the study. Session 2 provides an overview of the fundamental concepts necessary for understanding the subject matter. Session 3 delves into the research methodology employed. Session 4 presents the proposed implementation of this research and the architecture. Session 5 presents a comprehensive assessment to determine the viability of a proposed implementation across technical dimensions. Session 6 presents the findings and interprets their significance within the hypothetical use cases of the study. As the document draws to a close, the Conclusion section in Session 7 offers a concise summary of the research conclusions, and potential future research avenues stemming from this study's findings.

2 Literature Review

2.1 Distributed Ledger Technology (DLT) and Blockchain

Recent years have seen the emergence of blockchain and Distributed Ledger Technologies (DLTs), which are transforming data storage and transaction processing. It's crucial to recognize that although related, blockchain technology and DLT are distinct entities. DLT is a comprehensive term covering various technologies that facilitate secure, transparent, and decentralized record-keeping across a network of participants [1]. It involves the use of diverse mathematical structures to register transactions in a distributed database. The most used alternative to blockchain as DLT technology is the Directed Acyclic Graph (DAG) [29].

Blockchain is a fault-tolerant distributed ledger platform that achieves consensus in a large, decentralized network of distrustful parties, enhancing security and transparency in transactions and digital interactions [44]. Originating with Bitcoin, introduced by Satoshi Nakamoto in 2008 as a peer-to-peer cryptocurrency mechanism without intermediaries [46], blockchain reduces fraud and data manipulation risks. Smart Contracts on Blockchain, defining token characteristics and governance, are self-executing contracts activated upon consensus, ensuring transaction security and reliability [41, 63]. The exploration of DLTs reveals their vast potential in facilitating and regulating transactions, extending to real-world objects and rights. This integration enhances the value and accessibility of these objects by providing improved record-keeping security, transparency, and ease of fractionation.

2.2 Central Bank Digital Currencies (CBDCs)

Central Bank Digital Currency (CBDC) [9], which can also be a tokenized deposit [8], represents a new form of money, a digital extension of the fiat currency issued by a country. According to the World Economic Forum, 98% of global central banks are exploring CBDC to determine how to modernize the capabilities of and improve access to central bank money [64]. Twenty-four CBDCs are projected to go live by 2030.

Atlantic Council tracks CBDC projects worldwide [27] showing the advancement of interest in developing digital currencies. It shows that three countries have fully launched a CBDC: the Bahamas, Jamaica, and Nigeria. Nineteen of the Group of 20 (G20) countries are now in the advanced stages of CBDC development. In most countries with an advanced retail CBDC project, the access to CBDCs is intermediated, meaning they are distributed through banks, financial institutions, and payment service providers.

2.3 Unified Ledger

The concept of the Unified Ledger (UL) [8], as advanced by the Bank for International Settlements (BIS), represents a theoretical blueprint for a future financial market infrastructure built upon shared programmable platforms. Its core proposition involves the integration of various tokenized assets – encompassing central bank money (CBDC), commercial bank money (tokenized deposits), and potentially other financial or real assets – within a single, unified digital environment. Leveraging distributed ledger technology (DLT) and tokenization, the UL aims to overcome the fragmentation prevalent in today's financial system, where different asset types reside in separate silos, often requiring complex and inefficient processes for interaction. The inclusion of tokenized central bank money is posited as a crucial element, providing a risk-free settlement asset directly on the platform, thereby enhancing safety and finality.

This integrated architecture is designed to unlock significant enhancements in financial transactions and processes through inherent programmability enabled by smart contracts. The UL facilitates atomic settlement, allowing for the simultaneous and conditional exchange of multiple assets (e.g., Delivery versus Payment - DvP; Payment versus Payment - PvP) directly on the ledger, thus mitigating settlement and counterparty risks. By creating a common venue for diverse tokenized claims, the Unified Ledger framework seeks to improve operational efficiency, reduce transaction costs, increase transparency within its permissioned structure, and foster innovation by enabling the seamless composition of novel financial products and services built upon this integrated foundation.

2.4 Finternet

The concept of the Finternet [12], emerging from discourse by the Bank for International Settlements (BIS), envisions a future financial system architecture characterized by a network of interconnected regulated platforms, drawing parallels with the structure and impact of the internet. It represents a potential evolution beyond individual Unified Ledgers (ULs), conceptualizing an ecosystem where multiple ULs, alongside potentially other compatible financial infrastructures, are seamlessly linked through standardized protocols. This framework relies fundamentally on the tokenization of money (including central bank digital currencies and tokenized commercial bank deposits) and other assets, combined with robust interoperability mechanisms. The primary goal is to enable these distinct platforms, potentially operating under different technologies or governance models, to communicate and transact with each other securely and efficiently, thereby creating a cohesive global financial network.

This networked approach, termed Finternet, aims to leverage the benefits of programmability and composability inherent in tokenization and smart contracts on a broader, cross-system scale. By facilitating seamless value transfer and data exchange across interconnected ledgers, the Finternet model promises significant improvements in the efficiency, speed, and cost of financial transactions, particularly in the cross-border domain where fragmentation is currently most pronounced. Furthermore, it seeks to foster innovation by allowing third parties to develop and offer new financial services that can operate across the network, anchored by the trust provided by regulated entities and the availability of central bank money as a secure settlement asset. Ultimately, the Finternet represents a vision for a more integrated, resilient, and accessible global financial system built on open standards and public-private collaboration.

2.5 Interoperability

The advent of Unified Ledger (UL) concept presents a paradigm for integrating diverse tokenized assets, such as wholesale and retail Central Bank Digital Currencies (CBDCs) and tokenized commercial bank deposits, onto a single programmable platform. This consolidation aims to enhance efficiency, reduce settlement risk through atomic transactions, and unlock new financial functionalities within the ledger's boundaries. However, the practical realization of these benefits often hinges on the UL's ability to interact seamlessly with external systems, particularly other permissioned distributed ledger technology (DLT) environments or even traditional infrastructures operated by different entities under distinct governance frameworks. This necessity drives the critical requirement for interoperability: the technical and governance capability enabling secure and reliable communication, data exchange, and value transfer between the intrinsically integrated environment of the UL and disparate external permissioned systems, thereby preventing informational and transactional silos and fostering a connected financial ecosystem.

Achieving robust interoperability between a multi-asset UL and other permissioned platforms necessitates specialized solutions capable of bridging potentially heterogeneous technological stacks and trust assumptions. Solutions range from standardized, network-based approaches to bespoke integrations. For instance, decentralized oracle networks or dedicated cross-chain protocols like Chainlink's Cross-Chain Interoperability Protocol (CCIP) [23] offer generalized frameworks for secure messaging and token transfers across different blockchains, including permissioned variants, potentially leveraging cryptographic proofs and consensus mechanisms. Conversely, custom-built solutions using direct connectors, exemplified by specific integration tools like the conceptual Listrack solution [62], provide tailored, point-to-point links between specific systems. While standardized protocols may offer broader compatibility with public and network effects, custom connectors can be optimized for specific performance or security requirements between known counterparties, highlighting the diverse architectural choices available to enable fluid interaction across the burgeoning landscape of tokenized assets on distinct permissioned ledgers.

2.6 Rollups

Rollups [31] are a layer-2 scalability mechanism designed to enhance the performance of unified ledger platforms by moving the bulk of transaction processing off-chain. Through off-chain processing, transactions are executed outside the main ledger environment, significantly reducing computational load and congestion on the base layer. These transactions are then grouped through batching, a process in which numerous operations are aggregated into a single compact data structure. This batch is transmitted back to the Layer-1 ledger in a condensed format, capturing the essential state changes and metadata. By minimizing the amount of data written to the main chain while preserving the verifiability of each transaction, rollups improve data transmission efficiency and reduce on-chain storage requirements.

This architecture strengthens scalability, as it allows a much higher volume of transactions to be processed per second compared to Layer-1 alone. The security model remains intact by anchoring the final state and transaction proofs to the base layer, ensuring that off-chain execution cannot compromise the integrity of the unified ledger. Moreover, rollups contribute to lower transaction costs by distributing fixed on-chain fees across many bundled operations, and they enable faster transaction finality by decoupling execution from slower consensus mechanisms. In unified ledger systems—where the consolidation of diverse financial and non-financial assets into a single, interoperable framework is critical—rollups provide a high-performance solution that meets the demands of real-time processing, auditability, and institutional-grade security.

2.7 Zero Trust

Zero Trust Architecture (ZTA) is a cybersecurity paradigm [61] that assumes no implicit trust within a network, regardless of the origin of access requests. In the context of a Regulated Digital Multi-Asset Network (RTMN), ZTA requires that every access request, whether from users, devices, or services, undergoes rigorous authentication and authorization processes. This approach is particularly pertinent in environments dealing with sensitive financial and digital assets, where the integrity and confidentiality of transactions are paramount. The key principles of ZTA include continuous verification of trustworthiness, enforcement of least privilege access, and comprehensive monitoring of all activities. By integrating these principles, RD-MANs can ensure that only authorized entities have access to critical resources, thereby mitigating risks associated with unauthorized access or insider threats.

To strengthen the security framework, RTMNs can incorporate advanced technologies such as Confidential Computing, Post-Quantum Cryptography (PQC), Decentralized Digital Identity (DDI), and robust security and observability components. Confidential Computing enables the processing of sensitive data in isolated environments, ensuring that data remains encrypted even during computation. PQC prepares the infrastructure to withstand the potential future threats posed by quantum computing advances. DDI frameworks provide secure and verifiable identity management, reducing reliance on centralized authorities and enhancing user privacy. Additionally, implementing comprehensive security measures, including encryption of data at rest and in transit, multi-factor authentication, and real-time monitoring, ensures that all interactions within the network are secure and auditable. These combined strategies not only fortify the security posture of RTMNs, but also align with regulatory requirements, ensuring compliance and fostering trust among stakeholders.

2.8 Privacy-by-design

Privacy in a unified ledger environment that supports Central Bank Digital Currencies (CBDCs) and tokenized multi-asset instruments is a fundamental requirement for ensuring both regulatory compliance and the protection of confidential financial data. Unlike public blockchains, where transaction data is fully transparent, a unified ledger must enable selective disclosure, allowing only authorized participants to access sensitive information. This is particularly important in financial markets, where participants such as central banks, commercial banks, and asset managers require differentiated access based on their roles and regulatory obligations. In this context, privacy must be embedded "by design" into the system architecture, ensuring that only counterparties and designated authorities can observe or interact with transaction data, while maintaining the integrity and auditability of the ledger.

The concept of privacy-by-design in such systems also includes strict access controls based on cryptographic identity frameworks and decentralized identity models. Only entities that are directly involved in Delivery versus Payment (DvP) or Payment versus Payment (PvP) operations can view or validate relevant transactions. This ensures that, for example, a settlement between two banks involving a CBDC and a tokenized government bond remains private to those parties and any designated regulatory overseers. The system enforces these access controls at the protocol level, using embedded authorization policies and digital credentials, thus avoiding data leakage across unrelated participants in the network.

Asynchronous messaging is also a critical component of this privacy-preserving infrastructure. It allows counterparties to interact and coordinate across different time zones and operational windows without requiring continuous synchronization or full data visibility. Secure, signed messages are exchanged in a non-blocking fashion, enabling flexible orchestration of complex financial workflows. Combined with zk-rollups and privacy-centric architecture, asynchronous messaging ensures that transaction participants remain loosely coupled while the integrity and confidentiality of the underlying assets and exchanges are preserved. This design ultimately supports the goals of interoperability, scalability, and regulatory alignment in a unified ledger ecosystem.

2.9 Confidential Computing

Confidential Computing is a security-enhancing paradigm that enables the processing of sensitive data within hardware-based Trusted Execution Environments (TEEs) [35], ensuring that data remains protected not only at rest and in transit but also during computation. In a Zero Trust architecture [3], where no implicit trust is granted to any component within or outside the network—Confidential Computing plays a critical role in preserving data confidentiality, integrity, and sovereignty. It enforces strict isolation of code and data from the host operating system, hypervisors, and even cloud providers. This is particularly vital in a RTMN, where financial institutions, central banks, and other stakeholders require secure execution environments to manage and process high-value transactions and confidential digital assets.

Technologies such as AMD Secure Encrypted Virtualization with Secure Nested Paging (SEV-SNP) [35] exemplify the practical implementation of Confidential Computing. AMD SEV-SNP extends this isolation to entire virtual machines, encrypting memory and enforcing strict access controls even against privileged system components. In the context of an RTMN, these capabilities ensure that transaction validation, asset issuance, and regulatory reporting processes can be executed securely, without exposing sensitive information to unauthorized entities. By embedding Confidential Computing into the fabric of a Zero Trust framework, RTMNs can guarantee not only compliance with stringent regulatory standards, but also resilience against insider threats and advanced persistent attacks, thus fostering trust in digital asset ecosystems.

2.10 Quantum-safe and Quantum-secure

Post-quantum cryptography (PQC), also identified as quantum-resistant or quantum computing-proof cryptography, represents a pivotal area of research dedicated to formulating cryptographic algorithms resilient against attacks mounted by quantum computers [51]. The significance of PQC is understood by examining the current cryptographic landscape, where conventional systems secure communications by leveraging the computational intractability of certain mathematical problems, notably prime number factorization or the discrete logarithm problem, which underpin widely used RSA and elliptic curve cryptographic keys [39]. However, these specific mathematical structures, while challenging for classical computational paradigms, are susceptible to efficient resolution by quantum computers; for instance, Shor's algorithm can factor large integers in polynomial time [58], and Regev's algorithm offers further efficiencies for related problems [56], thereby undermining the security of contemporary cryptographic infrastructures. The ongoing substantial investment in quantum computing development by entities such as IBM, with projections for operational quantum computers within the next decade [45], underscores the imperative to establish secure cryptographic alternatives.

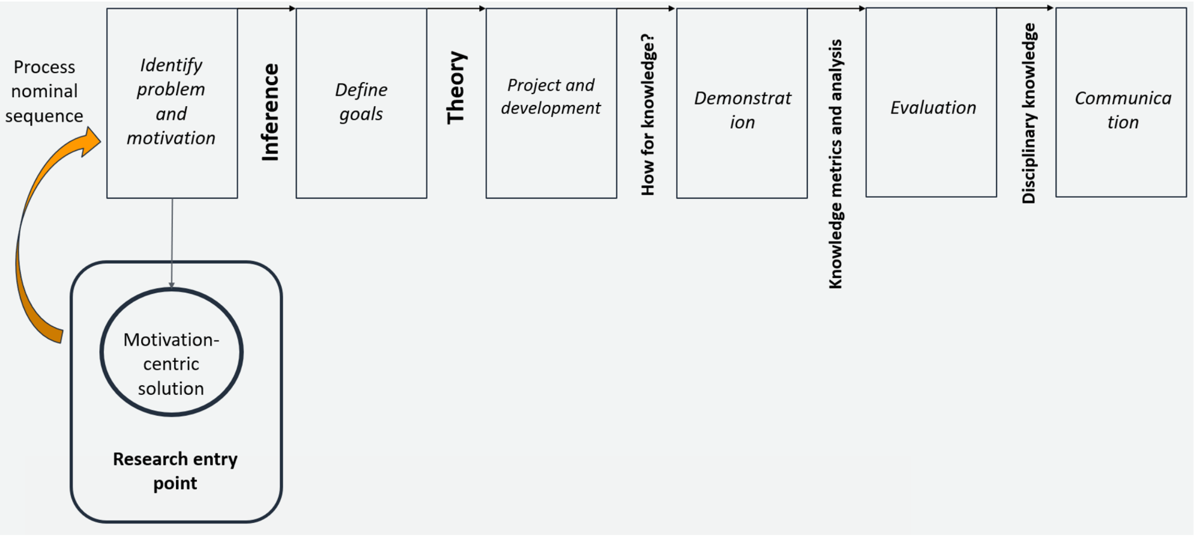
Within the discourse on cryptographic systems designed to withstand quantum computation, it is constructive to differentiate between the terms quantum-safe and quantum-secure. Quantum-safe typically denotes cryptographic algorithms and systems that are specifically engineered and, based on current understanding, are resistant to cryptanalysis by known quantum algorithms. In contrast, quantum-secure can be conceptualized as representing a more profound and ideally enduring level of security. This higher assurance might be theoretically grounded in principles akin to pattern-devoid cryptography, a paradigm aiming for cryptographic constructions that inherently lack the discernible mathematical structures, periodicities, or patterns that cryptanalytic algorithms quantum or classical are designed to exploit. A cryptographic system that rigorously adheres to pattern-devoid principles would derive its robustness from a fundamental randomness or structural unpredictability, rendering it intrinsically resilient to computational attacks that rely on identifying and leveraging such underlying regularities.

The proactive global response to the quantum threat includes significant standardization efforts, most notably by the National Institute of Standards and Technology (NIST), which initiated a comprehensive process to identify PQC algorithms [48]. This multi-year endeavor culminated in the selection of a first suite of algorithms in 2022, featuring CRYSTALS-Kyber for Key Encapsulation Mechanisms (KEMs), alongside CRYSTALS-Dilithium, Falcon, and SPHINCS+ for digital signatures [49]. These selected algorithms are categorized as quantum-safe, as their security foundations lie in mathematical problems such as those involving lattices, isogenies, hash functions, or multivariate equations that are currently believed to be resistant to efficient solution by quantum computers. While PQC standards may not achieve absolute pattern-devoidness in an information-theoretic sense, their design philosophies consciously eschew the specific structural properties vulnerable to known quantum attacks, thereby striving towards a state of practical quantum security and marking a crucial transition away from the cryptographic primitives of the pre-quantum era.

3 Methodology

The method adopted to support the making of this article is the Design Science Research Methodology (DSRM) [52] in its nominal sequence. This method includes six steps: (1) problem identification and motivation; (2) definition of the objectives of a solution; (3) design and development; (4) demonstration; (5) evaluation; and (6) communication, as we can see in Figure 2. The method allows the search to start at any of steps (1), (2), (3), or (4), and therefore the nominal sequence of the process may not be followed. For this work, the solution sought is centered on motivation and, therefore, its first nominal activity was number one, based on growing and market demand, in addition to the regulator BCB (Brazilian Central Bank) around Drex pilot [17], in addition to many other central banks.

Figure 2: *Nominal sequence of Design Science Research Methodology (DSRM).*



This chapter describes the applicability of DSRM to research about utilizing a framework to address asymmetries in the financial ecosystem and maintain privacy in an RTMN (Regulated Tokenized Multi-Asset Network), from demand confirmation to communication.

3.1 Demand confirmation

Within the complex and dynamic financial ecosystem of a nation such as Brazil, the implementation of a Central Bank Digital Currency (CBDC) utilizing permissioned Distributed Ledger Technology (DLT) confronts an amplified and critical imperative for robust privacy and confidentiality. The established cultural and regulatory expectations for financial secrecy among citizens and corporations, underpinned by frameworks like Brazil's *Lei Geral de Proteção de Dados Pessoais (LGPD)* [37], render the potential for granular transaction visibility inherent in some DLT models particularly problematic. Failure to adequately address this demand poses a severe risk, potentially undermining public trust not only in the CBDC itself but in the broader digital financial infrastructure, hindering adoption, and creating unacceptable vulnerabilities related to data misuse and surveillance within the Brazilian context. This underscores that the demand for stringent privacy guarantees is not merely a preference but a fundamental prerequisite for the operational viability and social acceptance of a CBDC in Brazil, thereby solidifying the necessity for a privacy by design architecture as the only tenable path forward, ensuring confidentiality is embedded systemically from the earliest stages of development. BIS [11] also reinforced the need for privacy in a CBDC platform.

3.2 Definition of goals

The fundamental objective of this work is to prove the feasibility of applying the proposed framework in a RTMN, and address privacy, atomicity, and finality in a distributed, composable, and programmable manner.

3.3 Design

The Motivation-Centered Solution was triggered by a real demand and can be treated with the development of a compartmentalized testing environment to apply the proposed framework with containers using confidential computing to address the Zero Trust concept, beyond asynchronous messaging.

3.4 Demonstration

This activity consists of defining the architecture of the standard off-chain environment based on containers, microservices, Kafka messages, and databases, in addition to the DLT environment (Besu) to represent the on-chain layer.

3.5 Evaluation

The assessment of the applicability of the integration will be carried out together with at least one financial institution to support one use case: tokenized federal government securities. It can be carried out later, through a pilot with them to implement the proposed framework, determine the integration flow, and determine which processes will be fully automated, in addition to the programmability, distribution, and privacy.

3.6 Communication

This white paper was prepared to be presented to the commercial banks and Central Banks. In this way, the practical results of this white paper will be shared with the Central Bank of Brazil and two financial institutions, primarily, before it is proposed for publication in the 7th Conference on Blockchain Research & Applications for Innovative Networks and Services [22].

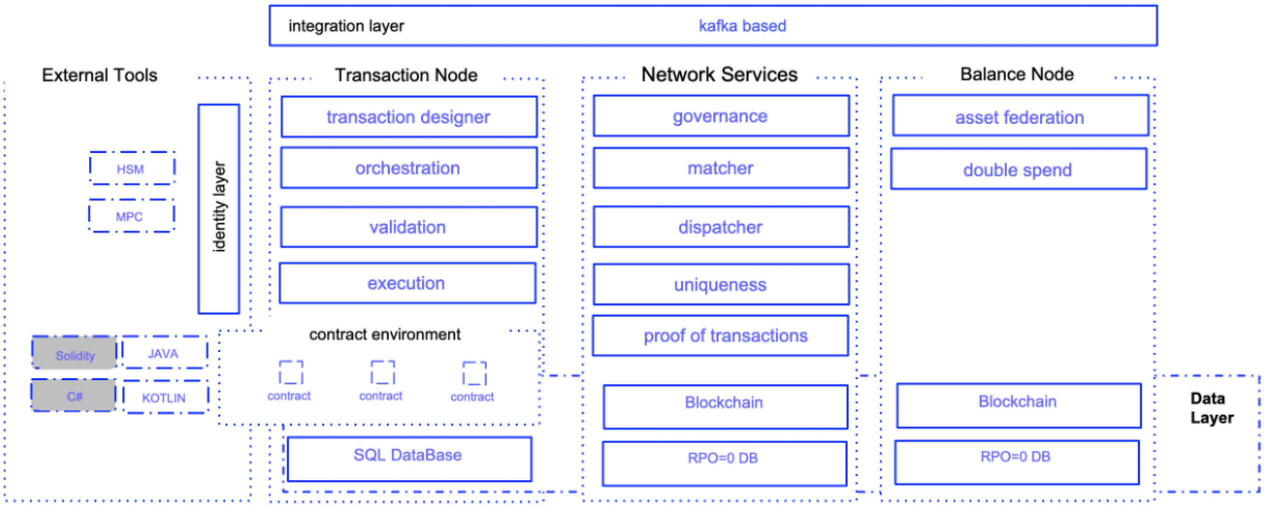
4 Implementation

This chapter describes the architecture of the proposed framework named Ptah applied to the Regulated Tokenized Multi-Asset Network (RTMN).

4.1 Architecture

The blueprint for the Ptah is detailed in Figure 3 with the following modules ("lego kits") distributed across different financial entities in a given financial ecosystem of a country or between them.

Figure 3: *Blueprint of architecture for privacy-by-design.*



A) Integration layer: Layer that is on top of the framework based on event streaming that is a data integration and processing paradigm where continuous streams of events are published to a platform (such as Apache Kafka) [2] and categorized into topics, enabling real-time data flow across distributed systems. It allows producers and consumers to be decoupled—systems that generate data don't need to know who will consume it, enhancing scalability, flexibility, and fault tolerance. By leveraging append-only logs and parallel processing, event streaming supports high-throughput, low-latency communication ideal for microservices and real-time analytics. The topic-based architecture enables efficient message routing and selective consumption, making it a powerful foundation for building responsive, event-driven architectures. More details in the subsection 4.2.3.

B) External tools: The integration of external tools into a RTMN is essential for enabling secure, compliant, and operationally scalable asset management. Specifically, the inclusion of digital asset custody infrastructures such as Fireblocks [34]' **MPC** (Multi-party computation)-based hot wallets and Dinamo [30]'s **HSM** (Hardware Security Module)-backed cold storage ensures cryptographic key control, transaction signing, and access policies are managed according to regulatory and institutional security requirements. MPC fragments private keys across multiple parties and environments, eliminating single points of failure and enabling secure, policy-driven transaction flows within the RTMN. Conversely, HSM provides hardware-enforced isolation and tamper resistance for storing private keys in offline (cold) environments, allowing RTMN participants to manage long-term, high-value assets with air-gapped security. These custody solutions can be natively integrated via standardized APIs (e.g., REST or gRPC) and cryptographic protocols (e.g., PKCS#11), enabling seamless key orchestration and transaction signing directly within the RTMN's transaction and settlement workflows. In parallel, decentralized identity (DiD) frameworks such as the one provided by CPQD [28] allow RTMN participants to establish self-sovereign, verifiable identities that are interoperable across ecosystems and anchored on distributed ledgers. These identities can be cryptographically linked to wallets, transaction endpoints, and access control mechanisms, enabling fine-grained authentication, authorization, and auditability without reliance on centralized identity providers. The RTMN can support multi-tenant identity governance, KYC (Know-Your-Customer) compliance, and on-chain reputation systems while preserving user privacy. The modularity of the RTMN data and identity layers allows for the seamless onboarding of DiD and custody providers through standardized interface contracts and protocol bridges, ensuring that financial institutions and regulated entities can plug in their preferred infrastructure components without compromising performance, interoperability, or compliance.

C) Data layer: Layer that is at the base of the framework, that consists of a cross layer between the framework modules and can be composed of at least three persistence technologies: **1)** The use of a Conflict-free Replicated Data Type (**CRDT**) [**CRDT**] database in a transactional environment is justified when low latency, high availability, and eventually consistent state must coexist with high performance in distributed architectures. CRDTs rely on mathematically defined data structures that guarantee convergence without requiring synchronous coordination, allowing for asynchronous replication and automatic conflict resolution. This makes them well-suited for cross-domain, cross-node architectures where multiple components such as transaction engines, balance state managers, and network orchestrators operate concurrently and in a loosely coupled manner. At the data layer, CRDTs enable local writes with guaranteed replication, drastically reducing user-facing latency and supporting deterministic eventual consistency, which is particularly useful for pre-validating balances, maintaining ephemeral state, or buffering transactions prior to commitment on the **DLT** (Distributed Ledger Technology) [42]. **2)** Alternatively, adopting a permissioned DLT as the authoritative balance state store offers cryptographic guarantees and immutability, making it ideal for use cases where auditability, non-repudiation, and inter-organizational synchronization are critical. The DLT acts as a single source of truth (SoT), ensuring that all balances and state transitions are derived deterministically from a tamper-evident transaction history, validated by a consensus mechanism. When integrated into the modular data layer, the DLT supports smart contract logic, decentralized authentication, and verifiable state computation, which is essential in regulated ecosystems or consortia. This model also simplifies compliance reporting and facilitates dispute resolution by enabling trustless verification of historical state. **3)** In addition to CRDTs and DLTs, incorporating a high-performance **SQL** [26] database at the transaction node provides a robust foundation for orchestrating and validating smart contracts. SQL databases offer deterministic, ACID-compliant (Atomicity, Consistency, Isolation, and Durability) transaction execution and support complex querying, which are advantageous for real-time contract execution, fee computation, and execution traceability. By decoupling transaction orchestration and logic execution from state persistence layers (CRDT or DLT), the SQL database functions as a fast, transactional runtime environment. This tri-layered architecture: SQL for deterministic orchestration, CRDT for low-latency pre-state handling, and DLT for canonical state and auditability enables modularity, scalability, and resilience across the entire transaction and balance management pipeline.

D) Transaction node: Node responsible for transactional flow, validation, orchestration, and execution:

- *Transaction designer*: Service responsible for obtaining all movements included within a transaction. The objective of the transaction designer is to access local (contract environment) and remote contracts, obtaining the list of movements that will later be submitted for validation.
- *Orchestration*: Service that requests the execution of operations on remote nodes. Among the operations we have the request to send competent transaction legs to each custodian and the execution of smart contract methods.
- *Validation*: Service that collects signatures from participants responsible for authorizing part or all of a transaction using specifics local or remote validation contracts that enforces bussiness rules.
- *Execution*: Service responsible for orchestrating a **Two-Phase Commit (2PC)** [36] operation between the balance bases involved in a single transaction.
- *Contract Environment*: Financial institution environment that permeates the external environment for the logic of smart contracts, with development tools, for example, in different programming languages such as Java, Kotlin, and in the future support to C# or Solidity via transpiler.

E) Network services: Services responsible for governance (mapping), association, dispatching, uniqueness, and proof of transactions:

- *Governance*: Service that stores routes and addresses of framework services; it is also responsible for indicating who is responsible for each type of component present in the network. Thus, the service supports distributed network governance.
- *Matcher*: Service that accumulates the signatures present in a transaction. The Matcher has visibility of which keys are involved in a transaction, but does not know what is being negotiated and its volumes. When it validates the presence of all keys, it informs the dispatcher that the transaction is authorized for execution.
- *Dispatcher*: Service that accumulates movements that are present in a transaction. The Dispatcher only knows that there are movements directed to specific balance bases, without knowing who the movements are from or what asset the movements are about. When it collects all the movements and receives authorization from the Matcher, it sends the transaction to the Transaction Pool.
- *Uniqueness*: Service for interoperability with the traditional market. It is the mechanism used to ensure that an asset that was not issued on the network will be unique when transported to this new architecture.
- *Proof of transactions*: Transaction finality disclosure base. Once a transaction is finalized, it is sent to this service so that all nodes involved in the transaction can apply the updates to their internal bases. At this point in the framework, it is possible to optionally use a rollup for proof generation, such as a ZK-EVM [54].

F) Balance node: Service that ensures that debits and credits from a single key are executed in the order of request, and that the balance is never negative (<0). The Balance Node only knows keys and balance, without knowing who the owner is and what the asset is. All operations executed against a Balance Node must follow a Two Phase Commit (2PC) protocol, to guarantee that all Balance Nodes involved in a single transaction also comply with the proposed movements. The choice of Balance service is defined by the asset issuer and may impact the performance of transactions involving that asset.

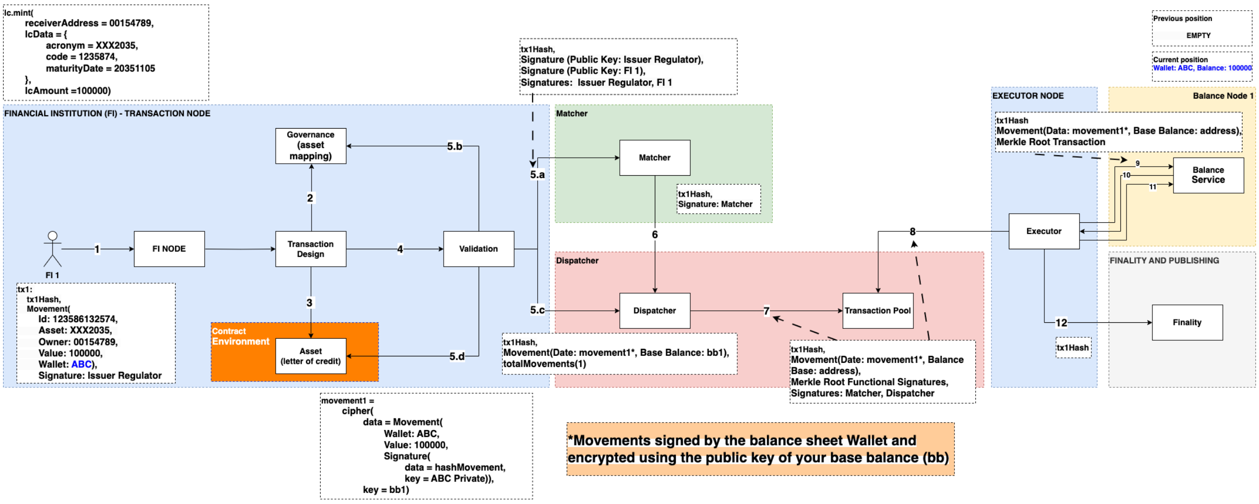
- *Asset Federation*: Each Balance node can be managed by a different federation, assets created within the network can be directed to a specific federation. The data must be in a balance node that is within a federation, for example, data from the Brazilian financial system must be within the Federation of a country like Brazil, the data must reside within databases in Brazilian territory. Even in the same country, others regulators could consider create an asset federation related to the current regulation.
- *Double spending*: The balance bases guarantee the order in which transactions are applied. Thus, only one transaction is executed per balance that it controls, thus ensuring that there will be no double spending.

4.2 Details of Architecture

Figure 4 represents the operational model of the Ptah framework, according to each phase: **1) validation**; **2) matching and aggregation**; **3) execution**; **4) finalization**; in addition to **5) segregation of responsibilities**. The step-by-step process is described below:

1. Send Mint Request.
2. Query route for involved contracts (e.g., letter of credit [lc] contract).
3. Request list of movements.
4. Send list of movements for authorization.
5. Validation: the framework does not know the owners of the public keys, and the keys used to sign the movements are different from the keys that are in the transaction, where there is a separation of identity key and balance key.
    (a) Send Signatures to Matcher service. The framework forces the separation of visibility for the Matcher: it has visibility of who needs to sign a transaction, without knowing what is being negotiated and its volumes.
    (b) Confirm list of authorizers in Governance module.
    (c) Send movements to Dispatcher service - it knows that there are movements, without knowing what is being negotiated or who is negotiating.
    (d) Send transaction for validation.
6. Confirm signatures.
7. Place transaction in execution pool.
8. Pooling in execution pool from Executor node.
9. Reservation Request - (two-phase commit).
10. Reservation confirmation - (two-phase commit).
11. Commit and confirmation - (two-phase commit).
12. Confirm transaction through rollup with finality.

Figure 4: *Operation process of Ptah framework.*



```
lc.mint(
    receiverAddress = 00154789,
    lcData = {
        acronym = XXX2035,
        code = 1235874,
        maturityDate = 20351105
    },
    lcAmount =100000)
```

```
tx1:
  tx1Hash,
  Movement(
     Id: 123586132574,
     Asset: XXX2035,
     Owner: 00154789,
     Value: 100000,
     Wallet: ABC),
     Signature: Issuer Regulator
```

```
movement1 =
    cipher(
        data = Movement(
            Wallet: ABC,
            Value: 100000,
            Signature(
                data = hashMovement,
                key = ABC Private)),
        key = bb1)
```

```
tx1Hash,
Signature (Public Key: Issuer Regulator),
Signature (Public Key: FI 1),
Signatures:  Issuer Regulator, FI 1
```

```
tx1Hash,
Signature: Matcher
```

```
tx1Hash,
Movement(Date: movement1*, Base Balance: bb1),
totalMovements(1)
```

```
tx1Hash,
Movement(Date: movement1*, Balance
Base: address),
Merkle Root Functional Signatures,
Signatures: Matcher, Dispatcher
```

```
tx1Hash
Movement(Data: movement1*, Base Balance: address),
Merkle Root Transaction
```

```
tx1Hash
```

```
Previous position
EMPTY
```

```
Current position
Wallet: ABC, Balance: 100000
```

*Movements signed by the balance sheet Wallet and encrypted using the public key of your base balance (bb)

The next subsections detail the functional characteristics of the Ptah framework applied to RTMN.

4.2.1 Privacy by design

Ptah adopts a privacy-by-design paradigm rooted in a distributed architecture with visibility and processing limited strictly to what is necessary. This architectural principle ensures that each network component operates with a minimally sufficient information set required to perform its role, eliminating unnecessary data exposure. In this model, only the transaction execution layer responsible for ensuring the finality through a 2PC protocol has access to the complete transactional context, including the identities of participants and the assets involved. All other services in the transaction lifecycle, including validation, matching, and dispatching, function over abstracted, de-identified data, thereby enforcing strict data isolation and privacy boundaries.

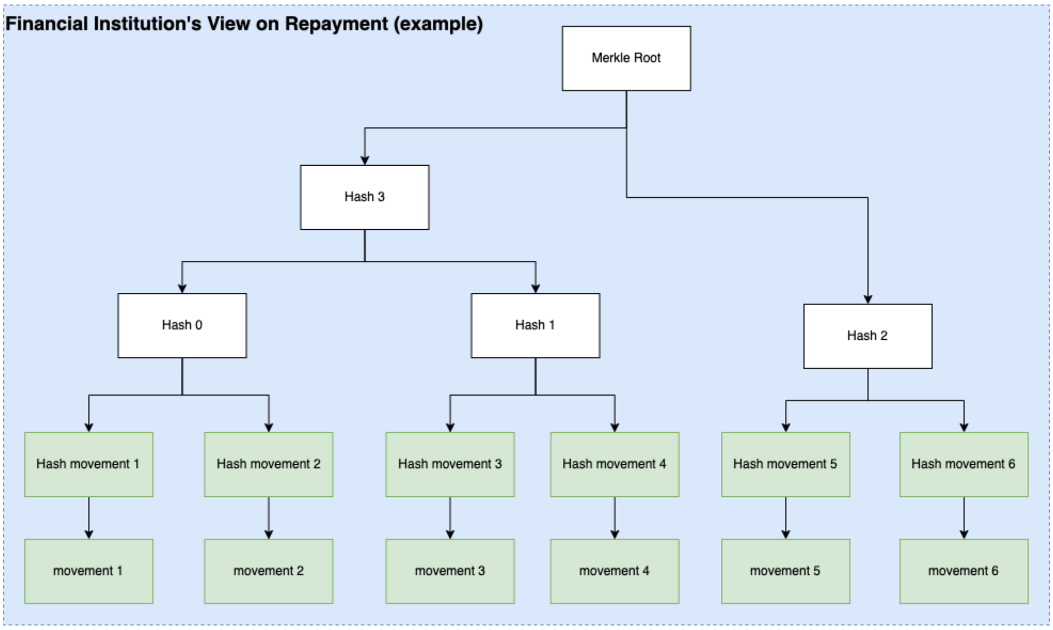
During the matching phase, the Matcher Service processes only the digital signatures and authorization metadata required to validate the eligibility of the transaction. It is intentionally unaware of the transaction semantics, such as asset class, amount, or wallet linkage, thus preventing any inference about the underlying financial intent. The Dispatcher Service, on the other hand, has visibility into movement instructions (e.g., wallet addresses and balance deltas) but remains agnostic to asset type and ownership. This orthogonal segregation of knowledge domains ensures that no individual service, except the designated executor, can reconstruct a complete view of the transaction state. Such compartmentalization significantly reduces the risk surface for data leakage and mitigates internal and external observability threats.

Through this design, RTMN achieves confidential, atomic, and auditable transaction execution within a regulated infrastructure. The selective exposure of data to only those services with a legitimate operational need, underpinned by cryptographic guarantees and formal access boundaries, enables institutional-grade privacy without compromising transactional correctness or composability. The architecture aligns with the requirements of multi-party financial systems, where trust is distributed and data sovereignty is paramount. This privacy-preserving modularity is not an add-on, but a foundational attribute of the RTMN protocol stack, enabling scalable, compliant deployment across heterogeneous financial actors.

4.2.2 Transaction verification

Each asset issued within the network can be marked by its issuers with authorization obligations whenever they are moved. Every balance movement, whether positive or negative, necessarily needs to be signed by its private key and by all the authorizers involved. Movements that do not have all the authorizing agents as signatories are not authorized within the Matching process. Thus, the process of validating a transaction involves signing a Merkle Root [6] of all the movements that are present in its context. To perform this operation, all the agents that need to authorize a transaction need to sign with their wallets that represent their identity the Merkle Root generated by a specific request.

Figure 5: *Merkle Root and movement hashes of a Financial Institution (repayment case).*



In DvP scenarios between two or more parties, there is no need for orchestration by one of the agents, since this transaction needs to be requested by each of these parties and everyone already needs to be in possession of all the data of the parties involved at the time of negotiation; thus, everyone already knows the movements that will be generated for each identity. Although DvP operations are the basis of the platform, most of the time, operations managed by smart contracts can stimulate third-party wallets where their custodians operate passively, waiting for a stimulus from the platform to send their leg with their specific movements. For example, in a context of repayment of a security that was partitioned and negotiated by several network participants, it always intends to make all payments atomically on the platform, to ensure the viability of the entire operation. This generates movements in which we expose the amount that will be paid to each identity involved. In order for each party to trust the integrity of the information, it needs a mechanism that enables verification by the receiving party of the balance, without exposing the other movements to the other identities, in order to maintain the privacy of the other participants.

To solve this problem, on the Ptah framework, there is no delivery of all the movements, but of each hash that is involved in this scenario, in addition to sending which movements are considered within the transaction. As can be seen in Figure 5, it is possible to calculate the same Merkle Root based on the hashes received plus the calculation of the hashes of only its transactions. In this way, all movements that are occurring within the transaction can be validated by whoever has possession of it, and the signature by all parties implies that all movements are considered valid, as long as the signed Merkle Root is the same for all parties, for example, custodian financial institutions one and two, as shown in Figures 6 and 7, respectively. Any change made within the context of a movement would generate a new Merkle Root, which would make it impossible to collect movements in the Dispatcher Service.

Figure 6: *Merkle Root of a Custodian Financial Institution 1.*

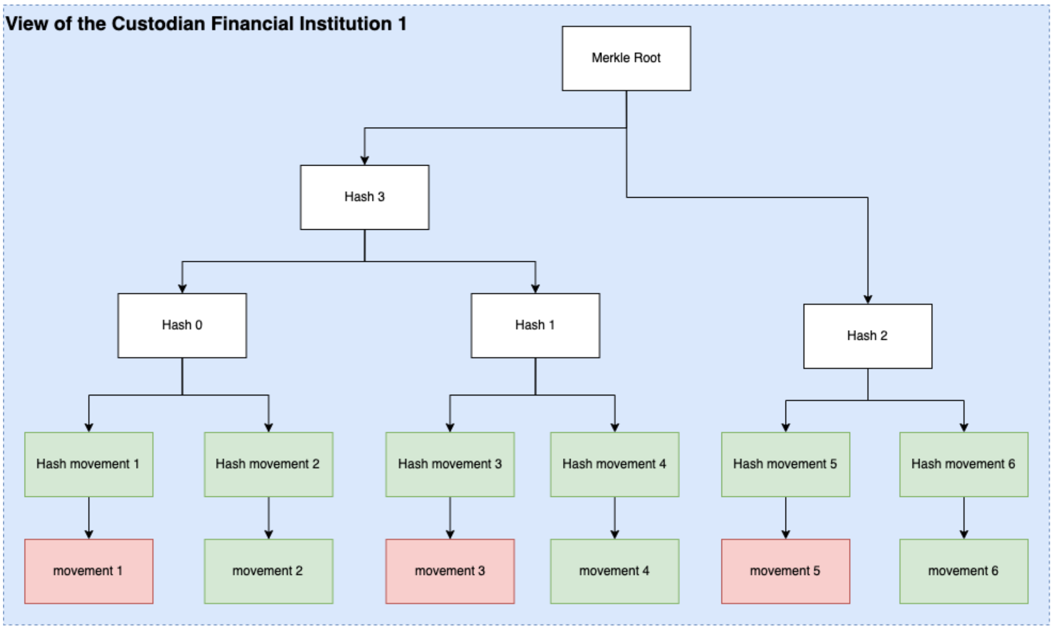
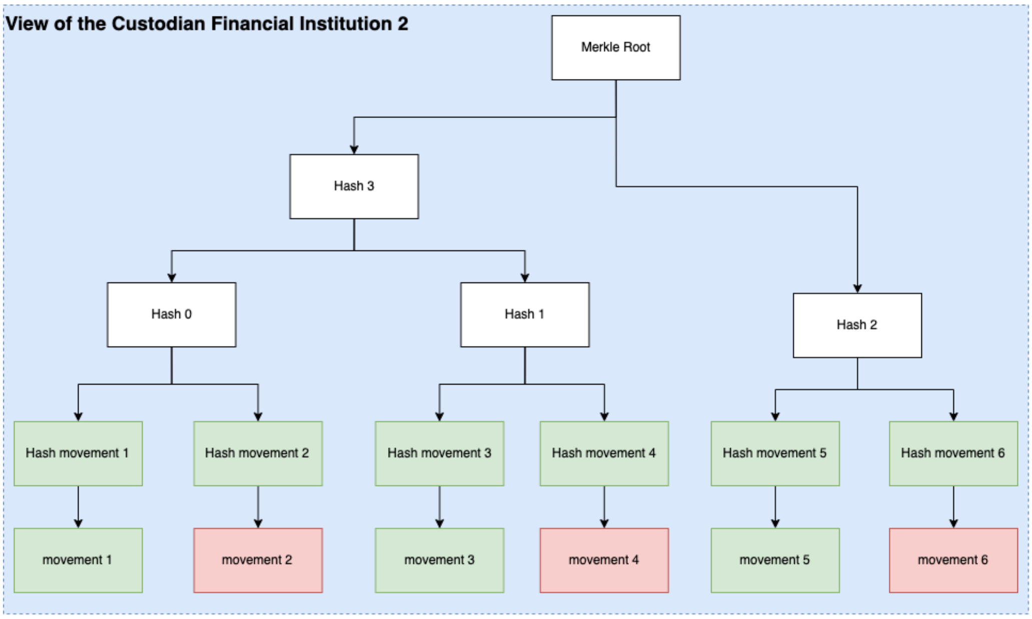


Figure 7: *Merkle Root of a Custodian Financial Institution 2.*



4.2.3 Asynchronous messaging

In the Ptah, asynchronous messaging serves as a foundational construct that decouples the temporal and logical dependencies between participants, enabling non-blocking coordination across diverse institutional domains. Unlike synchronous communication models, which require both parties to be simultaneously available and state-aware, asynchronous messaging introduces temporal independence, allowing entities to issue, receive, and process messages according to their operational windows and internal consistency guarantees. Messages exchanged across the network are cryptographically signed, timestamped, and integrity-verified, ensuring authenticity, non-repudiation, and replay protection. These guarantees are vital in a regulatory environment where transaction traceability and auditability are not only functional requirements but also legal imperatives. Furthermore, this messaging infrastructure is tightly integrated with fine-grained access control layers, ensuring that only authorized endpoints can consume or act upon specific messages, thereby preserving the confidentiality and integrity of bilateral or multilateral workflows.

The architectural adoption of asynchronous communication also underpins the privacy-by-design and resilience objectives of RTMN. By avoiding shared global state exposure and eschewing centralized orchestration, the system limits the amount of context each actor must disclose, thereby minimizing metadata leakage and systemic observability. For instance, in multi-party workflows such as DvP or asset swaps, counterparties may use asynchronous messaging to submit partial transaction legs, pre-authorization artifacts, or intent declarations. These are then selectively assembled and orchestrated into executable transactions by independent services (e.g., orchestrators, matchers) without requiring direct, synchronous coupling between all involved actors. This messaging substrate, therefore, not only facilitates composability and cross-domain coordination but also supports fault-tolerant execution, as it decouples availability from finality. In high-assurance environments like CBDC-enabled ecosystems, where fault isolation, auditability, and transaction atomicity must coexist, asynchronous messaging enables robust, secure, and privacy-preserving distributed state transitions.

4.2.4 Multi-assets

Ptah integrates multi-asset functionality directly at the settlement layer through a unified asynchronous messaging infrastructure designed to coordinate atomic and final settlement across heterogeneous execution environments. This design enables interoperability between various regulated tokenized instruments, including tokenized central bank deposits, commercial bank deposits, tokenized securities, and other compliant digital assets within a common settlement venue. Settlement finality is ensured through orchestrated message-driven workflows, which are capable of triggering deterministic execution on a range of supported back-end infrastructures. These may include DLTs such as Ethereum Virtual Machine (EVM), high-performance relational databases, or distributed SQL platforms like CRDT (active-active database), depending on institutional requirements for performance, auditability, or compliance.

This multi-asset architecture, derived from the BIS's Unified Ledger [8] and Finternet [12] frameworks, is purpose-built for extensibility, supporting a broad spectrum of asset types and transaction volumes while maintaining resilience and regulatory alignment, such as debentures, RWAs (Real World Assets), letters of credit, among others. By decoupling the orchestration layer from the settlement execution engine, the RTMN offers infrastructure modularity allowing financial institutions to select settlement environments based on specific use case constraints such as throughput, privacy, latency, and jurisdictional mandates. This flexibility enhances the versatility of the network, enabling seamless integration of future asset types and promoting innovation within regulated digital finance. Ultimately, the RTMN using Ptah provides a scalable and compliant foundation for comprehensive multi-asset settlement, whether deployed over decentralized or centralized execution environments.

4.2.5 Distribution

Ptah implements a distributed architectural [10] model in which each financial institution operates its own independent cluster of transaction nodes, responsible for the orchestration, execution, and validation of digital asset workflows. This model avoids reliance on any central processing authority, distributing both computational load and governance responsibilities across a federation of institutional participants. While certain network services such as identity resolution remain institution-specific, key protocol-level services like **Dispatcher, Matching**, **Governance**, and **Balance Management** are implemented as network distributed services, enabling deterministic behavior without requiring centralized trust anchors. This topology promotes fault isolation, ensures institutional autonomy, and allows for localized compliance and data sovereignty while still participating in a globally consistent settlement network.

This distributed configuration also supports the inclusion of multiple stakeholder classes, including central banks, regulatory bodies, and commercial financial institutions, each running nodes that integrate seamlessly into the RTMN stack. Crucially, the network's consensus and coordination logic is designed to operate over heterogeneous trust domains, allowing each node to independently verify the subset of state transitions relevant to its jurisdiction without requiring access to the full global ledger. The design enforces horizontal scalability and institutional compartmentalization, while still preserving atomic cross-institutional settlement through protocol-level coordination (e.g., via the Two-Phase Commit protocol). This distribution not only enhances network resilience and transparency but also aligns with regulatory requirements for non-custodial infrastructure and multi-party governance, positioning Ptah as a robust backbone for the next generation of compliant digital financial markets (RTMNs).

4.2.6 Modularity - "lego kits"

Ptah is architected as a modular system of interoperable microservices, where each component fulfills a discrete function within the lifecycle of digital asset transactions. This modularity resembles a “Lego kit” model, allowing independent units such as transaction and balance nodes and network-level matchers to be composed and reconfigured based on institutional requirements. The Transaction Node, which serves as the interface between financial institutions and the network, exemplifies this design. It is decomposed into specialized microservices such as the Transaction Designer, which retrieves and assembles the necessary movements to fulfill a transaction, and the Transaction Orchestrator, which coordinates the network-wide interaction required to aggregate complementary transaction legs from counterparties. This separation of concerns enhances maintainability, scalability, and adaptability, while ensuring strict protocol adherence.

Central to the modularity of Ptah is the Transaction Executor, a microservice responsible for ensuring transactional finality through the 2PC protocol. The executor interacts directly with Balance Services, each of which independently manages wallet balances without knowledge of wallet ownership or asset metadata. Upon successful coordination and execution, the transaction produces a cryptographic proof of finality, which can be broadcast for regulatory or audit purposes. Alongside this, the **Data Layer** facilitates the bilateral exchange of sensitive information such as anti-fraud, terrorism, and money laundering data between institutions, without leaking this data to the broader network. This separation of execution, orchestration, and information governance allows each function to evolve independently while preserving strong inter-service contracts, a hallmark of modular system engineering.

At the network layer, modularity extends beyond individual transaction nodes. Services such as the **Governance, Matcher, and Dispatcher** operate as decoupled validators of various aspects of a transaction. The Governance service resolves custodianship and identifies the institution responsible for each asset type; the Matcher validates that all necessary digital signatures are present without visibility into transaction content, while Dispatcher, with only access to the structure of the transaction, sequences it into the network upon Matcher approval. This compartmentalized knowledge model enhances security, privacy, and regulatory compliance. Furthermore, the Balance Service, entirely agnostic to asset identity and wallet ownership, embodies a generalized accounting engine that can be reused across asset classes. Through this design, RTMN achieves a flexible, institution-neutral environment in which new financial instruments, workflows, or regulatory constraints can be supported simply by rearranging or extending modular components.

4.2.7 Composability

In the Ptah, composability is a core principle that enables smart contracts to interact modularly and hierarchically, allowing complex financial workflows to be constructed from simpler, reusable components. This is achieved through a standardized, high-level interface for smart contract development, which allows a contract to invoke other contracts directly within the network. As a result, a smart contract can delegate responsibility for generating specific movements such as balance transfers or asset issuances to other trusted contracts. This modular design supports extensibility and code reuse, facilitating the implementation of multi-asset and multi-party logic in a scalable and maintainable manner.

A practical example of composability occurs in the case of an initial debenture offering. In this scenario, a centralized contract (the Offering Contract) orchestrates the financial settlement of the offering by triggering movement requests for a tokenized fiat asset (e.g., Tokenized Real [Drex]). The Offering Contract must be capable of identifying and interacting with the Real Token contracts of each participant involved in the transaction. It generates signed transaction proposals that instruct the transfer of tokenized currency, which, when validated, result in the issuance of debenture units to investors. This interaction happens entirely through smart contract logic, highlighting the ability of contracts to initiate actions on behalf of participants, provided they comply with the permissioning and custodial logic enforced on the network.

Critically, because wallet ownership and authorization remain under the control of custodians, the execution of such transactions depends on coordinated multi-node orchestration. While the Offering Contract may initiate the process, the custodial node associated with each investor must validate the authorization of the underlying movement. This is made possible through composability: the custodian's smart contract can autonomously verify the investor's consent and complete the "second leg" of the DvP operation. Such a model preserves decentralization of control while enabling synchronized, compliant transaction flows across institutional actors, making composability a foundational mechanism for building regulated, cross-asset financial applications on RTMN.

4.2.8 Atomicity

Ptah ensures atomic and consistent multi-asset transactions through the implementation of a distributed 2PC protocol across its Balance Services. Each transaction is coordinated by an **Execution Service**, which initiates a set of debit and credit operations involving one or more wallets. During the prepare phase, debit operations result in a temporary reservation of funds, ensuring that values are isolated but not yet deducted, while credit operations are recorded as pending movements that do not yet affect the recipient's balance. If all involved Balance Services confirm their ability to prepare, the transaction proceeds to the commit phase, finalizing the reserved debits and applying the pending credits. Otherwise, a rollback is triggered, releasing all reservations and discarding pending operations, thereby ensuring that all changes are either fully applied or fully canceled.

This architectural framework supports concurrent transactional workflows by maintaining strict separation between committed and in-flight movements. Funds under reservation cannot be double-spent, and pending credits are not prematurely visible, enabling safe parallel execution of operations across wallets and services. As a result, RTMN provides strong guarantees of atomicity, consistency, and isolation, even in the context of complex, multi-party digital asset transactions. This mechanism allows regulated financial networks to support interoperable and deterministic asset transfers, while preserving the integrity of wallet balances and the correctness of the distributed state.

4.2.9 Programmability

In the Ptah architecture, programmability is enabled through a clear separation between transaction authorization and execution, allowing for the composition and validation of complex financial logic across multiple layers. This model introduces two classes of programmable contracts: transaction generation contracts and transaction validation contracts. Generation contracts expose high-level, user-facing interfaces (e.g., transferFrom(from, to, value)) that abstract away low-level balance operations. These contracts translate abstract user intents into concrete Movements **(e.g., mv1(from, -value), mv2(to, +value))**, which the network can process. Moreover, these contracts can be compositional, enabling reusable logic, where one contract may invoke others to produce multi-asset, multi-step transactions with complex interdependencies, offering flexibility and modularity in transaction logic design.

Complementing this, validation contracts are responsible for asserting the logical correctness and policy compliance of proposed transactions, independent of participants' balances. These contracts examine the sequence of Movements within a transaction and determine whether they conform to the rules associated with the involved assets (e.g., regulatory constraints, risk controls, or business rules). Since a single transaction may involve multiple assets or jurisdictions, it can be validated by several independent sources across the network. This layered validation ensures domain-specific correctness while maintaining asset-agnostic transaction orchestration. The overall programmability of Ptah is further reinforced by the orchestration layer, which manages the invocation of generation and validation contracts and initiates the lifecycle of atomic transactions across the distributed network.

4.2.10 Interoperability

Interoperability is a foundational requirement for RTMNs, which envision a fragmented yet interconnected financial ecosystem comprising heterogeneous ledgers, institutional clusters, and sovereign digital asset infrastructures. As RTMN nodes represent distinct financial institutions, each potentially operating under unique technological stacks, regulatory jurisdictions, and trust models the ability to execute, validate, and synchronize state transitions across independent systems is paramount. This aligns with the broader paradigm of the Finternet (Financial Internet), which conceptualizes a global framework where unified ledgers interoperate through standardized protocols, enabling atomic asset exchange, policy enforcement, and cross-domain composability without requiring centralized mediation or relinquishing institutional control. In addition to asynchronous messaging between RTMN participants that enables interoperability and multi-asset exchange, other solutions could be coupled to the Ptah framework, such as Chainlink solutions or Listrack itself.

Chainlink's Cross-Chain Interoperability Protocol (CCIP) [23] enables secure data and token transfers across different blockchains. The Chainlink Runtime Environment (CRE) [24] is a broader execution platform for developers to build and run complex smart contract applications that can leverage various Chainlink services, including CCIP, and connect to off-chain systems. CCIP acts as a universal messaging and token movement bridge, allowing your decentralized applications (dApps) to interact seamlessly and securely with other chains. CRE provides a comprehensive, chain-agnostic environment to orchestrate and execute advanced workflows that combine on-chain logic with off-chain data and computation, simplifying the development of sophisticated, interconnected applications.

An alternative, deterministic model is exemplified by Lickstrack [62], which proposes a direct connector architecture for inter-ledger communication. Lickstrack integrates with each target environment via native RPC endpoints, SDKs, or ledger-specific APIs, deploying execution modules that transform transaction intents into valid, signed operations on the destination ledger. Within RTMN, a Lickstrack connector could, for instance, interpret a custody-side transaction for tokenized sovereign debt and propagate its settlement instruction directly into a corporate issuance network, where execution is finalized in accordance with bilateral policy contracts. Unlike oracle-based approaches, this method offers synchronous, low-latency interoperability and strong execution determinism, albeit at the cost of tighter coupling and bespoke integration logic. Together, CCIP and Lickstrack illustrate complementary strategies to enable secure, auditable, and compliant multi-ledger orchestration within and beyond the Ptah framework, making it especially suitable for interactions between RTMN and public-permissioned or permissionless infrastructures, such as tokenized collateral chains or international stablecoin rails.

4.2.11 EVM Compatibility

The Ptah framework's off-chain layer for RTMNs serves as the primary interface for user and system interactions, performing crucial pre-processing, and complex business logic before engaging the on-chain EVM DLT. This off-chain environment manages sensitive data, constructs and cryptographically signs transactions, and submits them to EVM nodes (like DLT Besu) via JSON-RPC to interact with smart contracts. Concurrently, off-chain services act as listeners, actively monitoring for events emitted by these smart contracts upon successful state changes. This event-driven approach allows the off-chain layer to synchronize its own state, update auxiliary databases, trigger subsequent business processes, and provide users or systems with timely feedback, creating a responsive and cohesive architecture that bridges off-chain operational complexities with on-chain assurances.

Depending on the defined architecture and required performance, some Ptah framework modules may benefit from a persistence module based on an EVM DLT. This bidirectional communication model is fundamental to these specific Ptah's modules: **a)** Balance Node leverages it by having off-chain systems initiate validated requests for asset movements, which are then atomically executed by on-chain token smart contracts. **b)** for Governance with asset mapping, off-chain workflows manage proposal deliberations and the collation of asset documentation; subsequent transactions then update on-chain governance rules to indicate responsabilities. **c)** finally, for the persistence of transaction proofs, Ptah's off-chain components collate evidence from complex operations and generate cryptographic summaries (like Merkle roots of audit data), which are then immutably recorded on the EVM DLT via smart contract interactions, providing a verifiable, timestamped anchor that supports robust auditing and regulatory oversight without placing all underlying data on-chain.

4.2.12 Security, Confidentiality and Quantum-resistant - Zero Trust Segmentation

Within the Ptah framework, particularly when extended to environments involving CBDCs, security is conceived under the Zero Trust paradigm [61], a model that inherently assumes no implicit trust across any entity, layer, or connection. In this context, traditional perimeter-based defenses are insufficient. Instead, the architecture mandates a layered enforcement of interlinked controls that span identity, access, network boundaries, and cryptographic guarantees. Central to this model is the notion of strong identity assurance, which involves continuous verification and multifactor authentication not only for human users but also for all digital actors, including devices, APIs, and microservices. Every request to access or process data must be explicitly validated in real time.

A second pillar of Zero Trust enforcement in the Ptah is the principle of least privilege, which restricts each entity human or machine to the minimal level of access necessary to perform its assigned functions, with time-bound scopes and strict revocation procedures. This is reinforced by microsegmentation, which isolates network and application components into discrete security domains, preventing lateral movement in the event of a breach. Each segment communicates only through rigorously monitored and policy-governed interfaces. In parallel, end-to-end encryption, both in transit and at rest, ensures data confidentiality and integrity, supported by enterprise-grade key management systems. Collectively, these controls safeguard the integrity of transactions, shield sensitive data from exposure, and mitigate the risk of sophisticated, targeted cyberattacks.

However, Zero Trust enforcement is incomplete without deep observability [53], which serves as the runtime feedback loop for validating that security controls are not only configured correctly but are functioning as expected. Observability within the Ptah involves real-time collection and correlation of telemetry across the entire stack spanning infrastructure, network, application logic, smart contract execution, and transactional flows. This continuous visibility enables the detection of anomalies and malicious behavior that may bypass static policy controls. It also empowers systems to detect violations such as privilege escalations, unauthorized access attempts, or irregular transaction propagation providing the operational context necessary for dynamic response.

To meet emerging cryptographic challenges, Ptah could integrates Post-Quantum Cryptography (PQC) primitives [38], ensuring that digital signatures, encryption schemes, and identity attestations are resistant to future quantum adversaries. In addition, Confidential Computing enclaves such as those based on Intel SGX [4] or AMD SEV-SNP [35] could be utilized to secure computation within hardware-isolated environments, ensuring that even privileged operators or infrastructure providers cannot observe in-memory transaction logic or key material.

4.2.13 High-Availability, Scalability and Performance

To ensure high availability and business continuity, the Ptah framework adopts a fundamentally stateless service architecture. This architectural paradigm enables rapid recovery and reallocation of computational responsibilities in the event of node-level failures during transactional execution. Specifically, should an active node fail mid-operation, a new instance can be provisioned with minimal latency, thereby resuming process execution without introducing significant service disruption. Furthermore, the forwarding of authorized transactions to multiple concurrent services, such as the Matcher and Dispatcher components, as well as the non-deterministic assignment of execution responsibility across participant nodes within the ecosystem, enhances systemic resilience. Nevertheless, the successful completion of distributed transactions remains contingent on the availability and responsiveness of third-party nodes, introducing an external dependency into the system's fault tolerance profile.

Scalability and performance are addressed through a distributed system architecture combined with the incorporation of advanced transaction processing techniques tailored for RTMNs. Notably, the framework includes support for rollups as a scalability layer, particularly for components interfacing with EVM-based DLTs, thereby significantly increasing throughput while maintaining verifiability. Additionally, the framework supports a heterogeneous persistence layer, comprising DLTs, CRDTs with a Recovery Point Objective (RPO) of zero, and ACID-compliant SQL databases enabling performance tuning and latency optimization in accordance with application specific requirements. These persistence options allow for the dynamic allocation of storage strategies based on the criticality, volume, and consistency demands of individual transaction classes.

The Ptah framework is intrinsically designed with distributed computing principles, a foundational requirement for achieving high availability, elasticity, and deterministic performance under variable load conditions. The synergy between stateless microservices, decentralized execution logic, and throughput-enhancing mechanisms such as rollups and asynchronous replication ensures that the system not only tolerates partial failures, but also dynamically adapts to fluctuating operational demands. This design enables the framework to meet the rigorous performance and continuity expectations of institutional financial infrastructures and decentralized finance (DeFi) environments, while maintaining a modular, extensible architecture aligned with regulatory and operational standards.

4.2.14 Finality

In the Ptah, finality refers to the deterministic and irreversible conclusion of a transaction's lifecycle, guaranteed through a combination of unique transaction identification, coordinated multi-party authorization, and atomic execution. Each transaction proposed within the network is assigned a globally unique identifier, which acts as a reference point to accumulate cryptographic signatures of authorization and execution from the various participants and services involved, including smart contracts, custodians, and identity providers. These signatures are systematically collected across modular components (e.g., Transaction Designer, Matcher, Executor), forming a verifiable audit trail that binds all stakeholders to the transaction intent. This identifier also serves as a concurrency control mechanism, preventing replay or duplication of operations once execution has been initiated.

Once a transaction reaches execution, its proposed movements to the atomic balance adjustments across wallets are committed via a distributed 2PC protocol. Upon successful completion of this protocol, the transaction achieves finality, rendering its state transitions immutable and its operations non-repeatable. A proof of execution, cryptographically derived and tamper-evident, is then propagated across the network, serving as an attestable artifact for audit, settlement, and regulatory compliance purposes. This finality mechanism ensures that the Ptah provides strong guarantees of transaction completeness and irreversibility, critical for regulated financial environments where legal and operational certainty is paramount. Exactly, at this point it is possible, optionally, to include a ZK-rollup solution [54] in order to generate proof of transaction execution, and verify them in the DLT layer, for example in the Besu DLT [42].

4.2.15 Pluggable ZK-rollup

The Ptah, by design, is modular and protocol-agnostic, capable of integrating diverse DLTs that vary widely in terms of transaction throughput (TPS), consensus latency, and state model complexity. In scenarios where certain nodes or edge domains such as public blockchains or legacy permissioned ledgers exhibit suboptimal performance characteristics, the network must employ auxiliary computational layers to preserve real-time responsiveness and transactional finality guarantees. To this end, Zero-Knowledge Rollups (ZK-Rollups) present a highly efficient cryptographic construct that can be optionally integrated into the Ptah architecture to batch, compress, and prove the correctness of off-chain transaction execution, thereby augmenting scalability without compromising data integrity or regulatory auditability.

ZK-Rollups operate by executing transactions off-chain within a dedicated rollup circuit or virtual machine, subsequently generating succinct Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs) [54], which serve as cryptographic proofs attesting to the correctness of the executed state transitions. These proofs, along with minimal state deltas, are periodically posted to an anchor ledger, which acts as the final arbiter for dispute resolution. In the context of Ptah, ZK-Rollups can be integrated as plug-in execution layers for high-volume subnets or asset classes, particularly in edge domains where native DLT layers cannot meet institutional TPS demands. By encapsulating thousands of transactions into a single cryptographic commitment, ZK-Rollups can reduce on-chain load, preserve deterministic settlement order, and ensure atomicity with significantly lower bandwidth requirements.

From a system integration perspective, these rollups can be deployed as co-processors or execution zones attached to transaction orchestration nodes within a Ptah cluster. These zones can process authorized movement proposals locally, generate zk-proofs for state transitions, and commit only final state roots and proofs back to the underlying DLT. The transaction orchestrator can then propagate this verified state to the broader Ptah services such as matcher and dispatcher, without requiring full exposure of transaction semantics. As DLT adoption accelerates across regulated domains, the pluggable integration of ZK-Rollups within RTMN offers a compelling pathway to resolve the scalability–compliance–privacy trilemma, enabling institutional-grade performance while upholding rigorous regulatory standards.

5 Feasibility Study

This Chapter describes the implementation challenges, regulatory adaptations, and application of Ptah in a specific use case: Tokenized Federal Public Securities.

5.1 Implementation challenges

The successful integration of a sophisticated security architecture, such as the Ptah framework, represents a pivotal step in advancing Brazil's Drex platform from its pilot phase to a production-grade Regulated Tokenized Multi-asset Network (RTMN). The framework's core tenet of cryptographically enforced information compartmentalization directly addresses the nuanced privacy challenges that have been central to the Drex pilot discussions. Rather than posing a challenge to regulatory oversight, this approach offers the Brazilian Central Bank (BCB) the prospect of achieving compliance-by-design. The implementation necessitates a co-evolution of advanced **Regulatory Technology (RegTech)** that can perform supervisory functions through verifiable cryptographic proofs, thereby ensuring systemic stability and preventing illicit activities without requiring unmitigated access to raw data. The viability of Ptah's acceptance, therefore, hinges on demonstrating this symbiotic relationship, where its advanced privacy-preserving features enhance, rather than obscure, the integrity and transparency mandated by the central banking authority.

From the perspective of Brazil's incumbent financial institutions, the adoption of the Ptah framework constitutes a strategic imperative for navigating the emergent tokenized economy. The decision to integrate such a system transcends a simple cost-benefit analysis, representing instead a calculated investment in next-generation security infrastructure. The computational overhead associated with its advanced cryptographic methods is not a deterrent but a precisely calibrated trade-off for achieving unparalleled guarantees of security, privacy, and transactional finality. For Brazilian entities already operating within a highly dynamic digital payments landscape shaped by innovations like Pix [19] and Open Finance [18], embracing the Ptah paradigm would signify a commitment to maintaining a competitive edge and operational resilience. The framework's adoption is thus contingent upon a clear elucidation of its value proposition in future-proofing institutional operations against the complex threat vectors of a decentralized financial ecosystem.

Ultimately, the viability of the Ptah framework as the catalyst for Drex's transition to full production depends on the strategic alignment of its technological architecture with both regulatory philosophy and commercial incentives. Its inherent support for atomicity, composability, and programmability provides the technical foundation required to foster the vibrant ecosystem of DeFi applications envisioned for the Drex platform. A successful deployment would therefore be predicated on a collaborative construction of a unified implementation roadmap, one that harmonizes the framework's advanced capabilities with the BCB's supervisory requirements and the strategic objectives of participating financial entities. By meticulously calibrating these elements, the implementation of the Ptah framework within Drex has the potential not only to resolve existing pilot-phase challenges but also to establish a new global benchmark for secure, private, and programmable digital financial infrastructures.

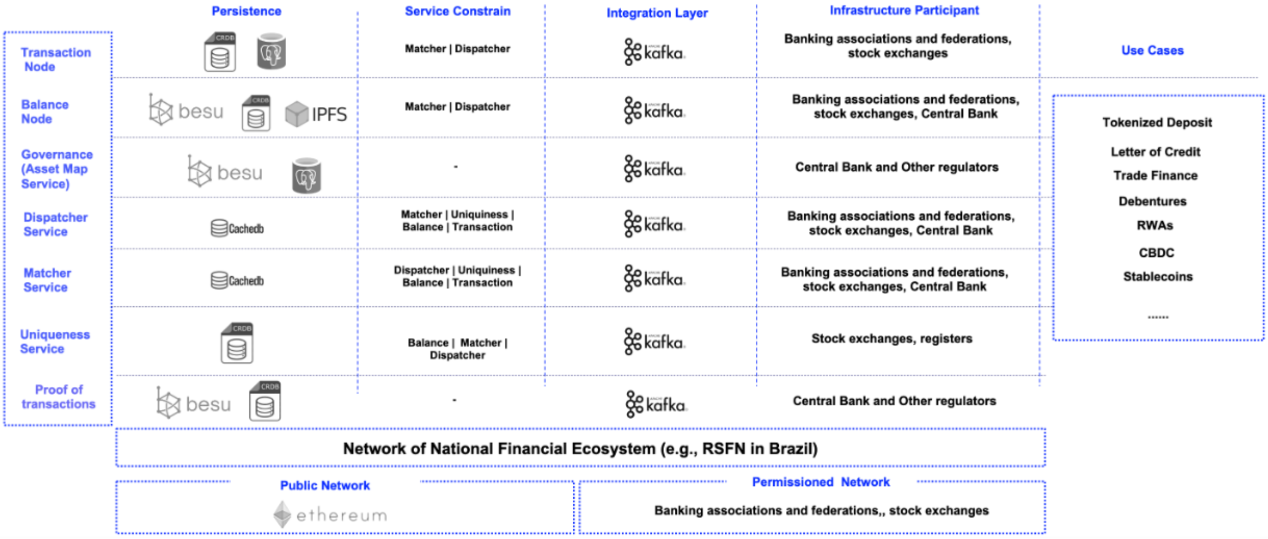
From a technological perspective, one of the main challenges in implementing Ptah in an RTMN lies in reconciling the inherent trade-offs between cryptographic privacy, functional compartmentalization, and system programmability. In RTMNs, particularly those involving CBDCs such as Drex, ensuring that architectural components operate with only the minimum necessary data can introduce complexities in orchestrating multi-party transactions, auditing workflows, and executing programmable financial instruments. These constraints require advanced cryptographic primitives such as secure multi-party computation, the integration of which often imposes significant performance and scalability costs, challenging the system's ability to meet the latency and throughput requirements of institutional-grade financial networks.

Another significant challenge concerns the implementation of Zero Trust principles in regulated DeFi environments. While Zero Trust architectures provide a conceptual foundation aligned with the distributed and borderless nature of DeFi, their practical deployment on RTMNs faces frictions related to regulatory compliance, performance assurance, and continuous auditability. For example, achieving the finality of real-time settlement and immutable record-keeping in a permissioned, multi-asset DeFi network requires a delicate balance between transparent data accessibility for regulators and rigorous privacy controls for participants. Ptah aims to overcome these challenges, and highlights the need for purpose-built frameworks that not only integrate robust cryptographic protections but also ensure seamless coordination among diverse actors under strict regulatory oversight. In this path of real implementation, the Figure 8 represents the hypothetical distribution of participants in a financial ecosystem, which would support each service of the Ptah framework, from brokerages, stock exchanges, payment institutions, commercial banks, central bank, other regulators, and issuers of tokenized assets.

5.2 Regulatory considerations

The implementation of the Ptah framework, as a foundational privacy-by-design architecture for Brazil's Drex platform, necessitates a sophisticated recalibration of the nation's core legal statutes governing data protection and financial confidentiality. Primarily, this involves reconciling Ptah's principles of cryptographic compartmentalization with the *Lei Geral de Proteção de Dados* (LGPD, Law No. 13,709/2018) [37] and the stringent Banking Secrecy Law (Complementary Law No. 105/2001) [20]. Current interpretations of the LGPD, which delineate the roles of data controllers and processors, are predicated on centralized data repositories. A regulatory evolution would be required to formally recognize decentralized architectures where data processing is minimized by design, potentially through amendments that validate the use of cryptographic attestations, such as Zero-Knowledge Proofs, as a legitimate means of demonstrating compliance. Concurrently, the Banking Secrecy Law would need to be modernized to incorporate a legal safe harbor for 'programmatic

Figure 8: *Hypothetical participants of a RTMN like Drex using Ptah.*



	Persistence	Service Constrain	Integration Layer	Infrastructure Participant
Transaction Node	CRDB	Matcher | Dispatcher	kafka	Banking associations and federations, stock exchanges
Balance Node	besu CRDB IPFS	Matcher | Dispatcher	kafka	Banking associations and federations, stock exchanges, Central Bank
Governance (Asset Map Service)	besu	-	kafka	Central Bank and Other regulators
Dispatcher Service	Cachedb	Matcher | Uniquiness | Balance | Transaction	kafka	Banking associations and federations, stock exchanges, Central Bank
Matcher Service	Cachedb	Dispatcher | Uniquiness | Balance | Transaction	kafka	Banking associations and federations, stock exchanges, Central Bank
Uniqueness Service	CRDB	Balance | Matcher | Dispatcher	kafka	Stock exchanges, registers
Proof of transactions	besu CRDB	-	kafka	Central Bank and Other regulators

Use Cases

Tokenized Deposit
Letter of Credit
Trade Finance
Debentures
RWAs
CBDC
Stablecoins
......

Network of National Financial Ecosystem (e.g., RSFN in Brazil)

Public Network
ethereum

Permissioned Network
Banking associations and federations,, stock exchanges

supervision', allowing the BCB to leverage embedded regulatory technologies that verify conformity with systemic rules without requiring direct access to underlying transactional data, thereby upholding the law's spirit while accommodating technological innovation.

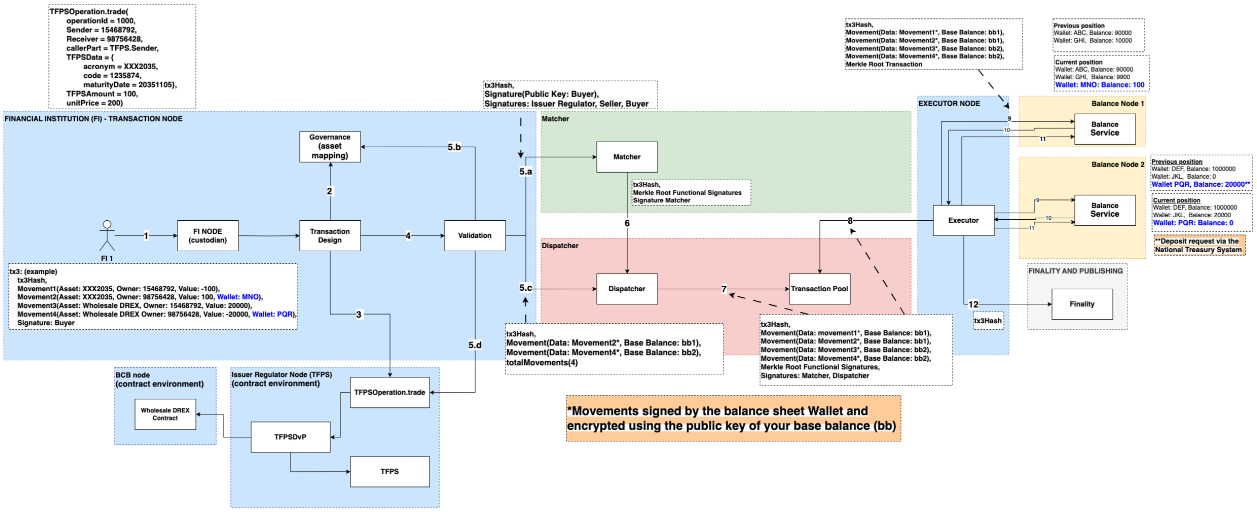
Beyond these foundational statutes, a second layer of regulatory evolution is imperative within the specific directives that operationalize Law No. 14,478/2022 (the Legal Framework for Virtual Assets) [21] and govern the National Financial System (NFS). As the cornerstone for digital asset regulation, this law provides the legal authority and definitions upon which the BCB and the *Comissão de Valores Mobiliários* (CVM) - Brazilian Securities and Exchange Commission must build their infra-legal norms. For the Drex platform to function, BCB regulations must evolve to detail how Virtual Asset Service Providers (VASPs), licensed under Law 14,478, will operate within a Ptah-enabled RTMN. This includes updating cybersecurity and operational risk frameworks (e.g., BCB Resolution CMN No. 4,893/2021) [5] to address DLT-specific risks and mandating formal verification for smart contracts handling the virtual assets defined by the new law. Furthermore, the concept of settlement finality must be legally cemented for DLT-based transactions involving these assets, ensuring that a cryptographically settled transaction is recognized as legally irrevocable, thereby providing market certainty and robust consumer protection as envisioned by the legal framework.

5.3 Analysis of the application in the case of Tokenized Federal Public Securities

The example in Figure 9 demonstrates Tokenized Federal Public Securities (TFPS) running on an RTMN, such as Drex, using Ptah. A trade transaction with TFPS (example tx3) is simulated, between a buyer and a seller, with movements of four balances, divided into two balance nodes, two of the TFPS asset and two of Drex Wholesale. Here is the step-by-step guide on the trade process with TFPS, detailed in Figure 9:

1. Sending purchase and sale steps.
2. Query for contracts involved (TFPSOperation.trade).
3. Request list of four movements.
4. Send list of movements for authorization.
5. Validation:
    (a) Send Signatures to Matcher service with Signatures of Issuer Regulator, Seller and Buyer. The framework designates accesses in the Matcher and Dispatcher calls, where the concept of **privacy-by-design** is employed. The Matcher has visibility of who needs to sign a transaction, without knowing what is being negotiated or its volumes. The Dispatcher only knows that there are movements, without knowing what is being negotiated or who is negotiating (5.c).
    (b) Confirm list of authorizers in Governance module (asset mapping).
    (c) Send encrypted movements to Dispatcher service.
    (d) Send transaction for validation. At this point, programmability is validated by calling at least four contracts in two other entities, with the Regulatory Issuer and the Central Bank (BCB, for example).

Figure 9: *Tokenized Federal Public Securities (TFPS) running on RTMN with Ptah.*


```
TFPSOperation.trade(
    operationId = 1000,
    Sender = 15468792,
    Receiver = 98756428,
    callerPart = TFPS.Sender,
    TFPSData = {
        acronym = XXX2035,
        code = 1235874,
        maturityDate = 20351105},
    TFPSAmount = 100,
    unitPrice = 200)
```

```
tx3: (example)
  tx3Hash,
  Movement1(Asset: XXX2035, Owner: 15468792, Value: -100),
  Movement2(Asset: XXX2035, Owner: 98756428, Value: 100, Wallet: MNO),
  Movement3(Asset: Wholesale DREX, Owner: 15468792, Value: 20000),
  Movement4(Asset: Wholesale DREX Owner: 98756428, Value: -20000, Wallet: PQR),
  Signature: Buyer
```

```
tx3Hash,
Signature(Public Key: Buyer),
Signatures: Issuer Regulator, Seller, Buyer
```

```
tx3Hash,
Merkle Root Functional Signatures
Signature Matcher
```

```
tx3Hash,
Movement(Data: Movement2*, Base Balance: bb1),
Movement(Data: Movement4*, Base Balance: bb2),
totalMovements(4)
```

```
tx3Hash,
Movement(Data: movement1*, Base Balance: bb1),
Movement(Data: Movement2*, Base Balance: bb1),
Movement(Data: Movement3*, Base Balance: bb2),
Movement(Data: Movement4*, Base Balance: bb2),
Merkle Root Functional Signatures,
Signatures: Matcher, Dispatcher
```

```
tx3Hash,
Movement(Data: Movement1*, Base Balance: bb1),
Movement(Data: Movement2*, Base Balance: bb1),
Movement(Data: Movement3*, Base Balance: bb2),
Movement(Data: Movement4*, Base Balance: bb2),
Merkle Root Transaction
```

```
Previous position
Wallet: ABC, Balance: 90000
Wallet: GHI,  Balance: 10000
```

```
Current position
Wallet: ABC, Balance: 90000
Wallet: GHI,  Balance: 9900
Wallet: MNO: Balance: 100
```

```
Previous position
Wallet: DEF, Balance: 1000000
Wallet: JKL,  Balance: 0
Wallet PQR, Balance: 20000**
```

```
Current position
Wallet: DEF, Balance: 1000000
Wallet: JKL,  Balance: 20000
Wallet: PQR: Balance: 0
```

**Deposit request via the National Treasury System

*Movements signed by the balance sheet Wallet and encrypted using the public key of your base balance (bb)

6. Confirm signatures: Issuer Regulator, Seller and Buyer.
7. Place transaction in execution pool. Here, the movements are signed by the balance sheet wallet and encrypted using the public key of your base balance.
8. Pooling in execution pool from Executor node.
9. Reservation Request - (two-phase commit). Stimulation on two balance nodes from the executor node: **1) MNO wallet** of the asset owner and **2) PQR wallet** of the Wholesale Drex owner. In the example of PQR wallet, the deposit request is via the National Treasury System (external regulator, for example).
10. Reservation confirmation - (two-phase commit).
11. Commit and confirmation - (two-phase commit).
12. Confirm transaction through rollup with finality.

6 Results and Discussions

As demonstrated in subsection 5.3, the Ptah framework is capable of supporting complex and high-stakes financial applications, such as the trading of Tokenized Federal Public Securities using Wholesale CBDCs. This capability stems from Ptah's foundational design principles, which prioritize privacy-by-design, composability, decentralization, and distributed architecture. These characteristics enable seamless interaction between multiple financial entities like commercial banks, central banks, stock exchanges while preserving an interoperable environment that bridges both off-chain and on-chain components. The framework's robust architecture positions it as a strategic enabler for programmable finance in scenarios demanding stringent compliance, trust minimization, and dynamic coordination.

Beyond performance metrics alone, the Ptah champions composability and programmability as core differentiators essential to supporting sophisticated financial infrastructures. In contrast to monolithic architectures, Ptah's modular design allows for granular integration, extensibility, and reuse of components across diverse applications and regulatory contexts. This approach fosters innovation and resilience, enabling financial institutions and technology providers to adapt quickly to evolving requirements. As financial systems grow more interconnected and policy-driven, the ability to compose and recompose services without compromising security or interoperability becomes a strategic advantage.

A compelling use case for Ptah is its potential integration with Unified Ledger [8] platforms, such as the Drex infrastructure currently under development. These platforms aim to consolidate Wholesale CBDCs, tokenized deposits, and a wide array of tokenized real and financial assets, including debentures, real estate, commodities like soybeans, and environmental assets such as decarbonization credits. In such ecosystems, Ptah addresses the paradox between interoperability and compartmentalization. It supports the operational and privacy requirements of complex jurisdictions, like Brazil, where regulatory and technological pluralism must coexist within a cohesive framework. This makes Ptah particularly suitable for projects requiring adaptable, secure, and interoperable financial infrastructures.

Ptah's relevance extends to global initiatives that are reshaping the foundations of digital finance, such as

BIS Innovation Hub projects including Agorá [13], mBridge [15], Hertha [14] to mitigate financial crime, and Leap [7] to be quantum-safe or quantum-secure. These initiatives require a framework that not only meets technical and operational benchmarks but also aligns with broader visions of financial inclusivity, sustainability, and innovation. Ptah's alignment with the Finternet [12] concept and the protopia movement illustrates its potential to be more than a technical substrate; it is a catalyst for building next-generation financial networks that are modular, programmable, and inherently cooperative.

Moreover, the Ptah framework is designed with the adaptability necessary to evolve into a comprehensive Zero Trust architecture. By incorporating confidential computing techniques, quantum-safe cryptographic algorithms, and hardware-enforced security modules, Ptah can meet the highest standards of cybersecurity and resilience. This evolution is not merely theoretical; it is technologically and operationally feasible, as its modular composition allows for the seamless integration of security enhancements without requiring a complete overhaul. In an era of increasing cyber threats, geopolitical fragmentation, and quantum computing advances, such adaptability is essential for the long-term trust and viability of digital financial infrastructures.

7 Conclusions

This Chapter describes the main advantages of using the Ptah framework and future work.

7.1 Advantages of the Framework

The Ptah framework constitutes a novel and comprehensive architectural foundation meticulously engineered to address the **multifaceted** requirements of Regulated Multi-Asset Networks (RTMNs), particularly those aligned with the BIS-driven vision of the Finternet. Ptah is uniquely positioned to enable both wholesale and retail CBDC deployments, tokenized deposits, stablecoins, and a wide range of real-world assets (RWAs) within an **integrated and programmable** financial ecosystem. It provides native support for **atomic and final settlement** mechanisms, leveraging a two-phase commit structure, while ensuring **cryptographic enforcement** of **information compartmentalization** across all components, in accordance with the **privacy-by-design** paradigm. Each architectural module operates under the principle of minimum necessary disclosure, a core prerequisite for sovereign-grade digital financial infrastructures.

Critically, Ptah reconciles the inherent trilemma faced in the implementation of tokenized financial platforms, namely **decentralization, privacy, and programmability**, without compromising the operational resilience or legal enforceability of transactions. It supports complex transaction patterns such as **DvP** and **PvP**, while maintaining comprehensive **compliance controls**, including asset mapping, rule validation, and **dynamic enforcement of jurisdiction-specific legal** and regulatory constraints. The framework also facilitates seamless **interoperability** between off-chain and on-chain environments, exhibiting both **technological agnosticism and high composability**, thus allowing modular integration with existing financial market infrastructures and distributed ledger platforms.

Designed with high **adaptability**, Ptah is inherently compatible with **Zero Trust** architectures, supporting quantum-safe cryptography, cryptographic agility, confidential computing, HSM integration, and MPC schemes for private key protection. Furthermore, its **scalability and performance** characteristics, enhanced by potential rollup integrations and parallel execution environments, render it suitable for **large-scale deployment** across heterogeneous financial ecosystems. Given these attributes, Ptah stands as a reference model for **secure**, interoperable, and privacy-preserving financial architecture, offering a viable blueprint for Central Bank initiatives seeking to modernize their infrastructures in alignment with **global multi-asset ledger** strategies.

7.2 Future Work

In considering the future of research on the domain of privacy-by-design and composability applied to Regulated Tokenized Multi-Asset Networks (RTMNs), several promising directions emerge that warrant exploration. Building upon the insights gained from the current study, potential areas for further investigation include the integration of quantum-safe algorithms, Zero-Knowledge Proofs (ZKP), account abstraction solutions [65], self-sovereign identity [43], in addition to interoperability with real-time payments (RTP) [19] and Open Finance [18] infrastructure based on ISO20022 [50], on-chain and off-chain anti-fraud/AMl/CFT solutions, and public networks like Solana [59], Polygon [55], Ethereum [32], etc.

The Ptah framework is currently being tested in phase 2 of the Drex (Central Bank of Brazil) pilot [16], with use cases related to international trade finance, tokenization of receivables and letters of credit, and the plan is to test it in other pilots in other countries and also in production.

References

[1] Ahmad J. Alkhodair, Saraju P. Mohanty, and Elias Kougianos. *Consensus Algorithms of Distributed Ledger Technology – A Comprehensive Analysis*. Accessed: 2025-03-05. 2023. arXiv: 2309.13498.

[2] Apache. *Kafka 4.0 Documentation*. https://kafka.apache.org/documentation/. Accessed: 2025-03-22. 2025.

[3] AWS. *Zero trust on AWS*. https://aws.amazon.com/security/zero-trust/?nc1=h_ls. Accessed: 2025-05-12. 2025.

[4] Azure. https://learn.microsoft.com/en-us/azure/confidential-computing/quick-create-portal. Accessed: 2023-12-20. 2024.

[5] Brazilian Central Bank. *Resolução CMN n° 4.893 de 26 de fevereiro de 2021*. https://cdn-www.bcb.gov.br/estabilidadefinanceira/exibenormativo=4893. Accessed: 2025-06-10. 2021.

[6] Binance. *Merkle Trees and Merkle Roots Explained*. https://academy.binance.com/en/articles/merkle-trees-and-merkle-roots-explained. Accessed: 2024-12-03. 2020.

[7] BIS. https://www.bis.org/about/bisih/topics/cyber_security/leap.htm. Accessed: 2024-04-10. 2024.

[8] BIS. *Blueprint for the future monetary system: improving the old, enabling the new*. https://www.bis.org/publ/arpdf/ar2023e3.pdf. Accessed: 2024-02-16. 2023.

[9] BIS. *Central Bank Digital Currencies*. Report 174. https://www.bis.org/cpmi/publ/d174.htm. Committee on Payments, Market Infrastructures, and Market Committee, Mar. 2018, p. 34.

[10] BIS. *Central bank digital currencies: System design*. https://www.bis.org/publ/othp88_system_design.pdf. Accessed: 2025-01-18. 2024.

[11] BIS. *Central Bank Digital Currency and Privacy: A Randomized Survey Experiment*. https://www.bis.org/publ/work1147.pdf. Accessed: 2025-27-04. 2023.

[12] BIS. *Finternet: the financial system for the future*. https://www.bis.org/publ/work1178.pdf. 2024.

[13] BIS. *Project Agorá: central banks and banking sector embark on major project to explore tokenisation of cross-border payments*. https://www.bis.org/press/p240403.htm. Accessed: 2025-03-16. 2024.

[14] BIS. *Project Hertha: Identifying financial crime patterns in real-time retail payment systems*. https://www.bis.org/about/bisih/topics/fmis/hertha.htm. Accessed: 2025-02-17. 2025.

[15] BIS. *Project mBridge reached minimum viable product stage*. https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm. Accessed: 2025-04-15. 2024.

[16] Central Bank of Brazil. *Banco Central do Brasil's - Innovation Agenda*. https://www.bcb.gov.br/conteudo/home-ptbr/TextosApresentacoes/Ap_RCN_Brunnermeier_3_10_24.pdf. Accessed: 2024-12-24. 2024.

[17] Central Bank of Brazil. *DREX*. https://www.bcb.gov.br/en/financialstability/drex_en. Accessed: 2025-06-09. 2024.

[18] Central Bank of Brazil. *Open finance*. https://www.bcb.gov.br/en/financialstability/open_finance. Accessed: 2025-06-10. 2025.

[19] Central Bank of Brazil. *Pix - Real-Time Payment*. https://www.bcb.gov.br/en/financialstability/pix_en. Accessed: 2025-06-10. 2025.

[20] Government of Brazil. *LEI COMPLEMENTAR N° 105, DE 10 DE JANEIRO DE 2001*. https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm. Accessed: 2025-06-10. 2001.

[21] Government of Brazil. *LEI N° 14.478, DE 21 DE DEZEMBRO DE 2022*. https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14478.htm. Accessed: 2025-06-10. 2022.

[22] UZH Blockchain Center. *7th Conference on Blockchain Research Applications for Innovative Networks and Services*. https://brains.dnac.org/2025/submissions/. Accessed: 2025-03-15. Zurich, SWI, 2025.

[23] Chainlink. *Cross-chain by Chainlink*. https://chain.link/cross-chain. Accessed: 2025-02-27. 2025.

[24] Chainlink. *Introducing Chainlink Runtime Environment (CRE): A Major Upgrade to the Chainlink Platform*. https://blog.chain.link/introducing-chainlink-runtime-environment/. Accessed: 2025-05-18. 2025.

[25] Chainlink. *What Is a Blockchain Oracle?* https://chain.link/education/blockchain-oracles. Accessed: 2025-04-03. 2025.

[26] Google Cloud. *Creating a high-performance SQL Server instance*. https://cloud.google.com/compute/docs/tutorials/creating-high-performance-sql-server-instance. Accessed: 2025-06-02. 2025.

[27] Atlantic Council. *Central Bank Digital Currency Tracker*. https://www.atlanticcouncil.org/cbdctracker. Accessed: 2025-05-14. 2025.

[28] CPQD. *ID CPQD*. https://www.cpqd.com.br/solucoes/id/. Accessed: 2025-06-02. 2025.

[29] Nathanaël Denis, Maryline Laurent, and Sophie Chabridon. "Integrating Usage Control Into Distributed Ledger Technology for Internet of Things Privacy". In: *IEEE Internet of Things Journal* 10.22 (Nov. 2023), pp. 20120–20133. ISSN: 2372-2541. DOI: 10.1109/jiot.2023.3283300. URL: http://dx.doi.org/10.1109/JIOT.2023.3283300.

[30] Dinamo. *Our Hardware Security Module (HSM) Family*. https://dinamonetworks.com/en/familia-hsm/. Accessed: 2025-05-25. 2025.

[31] Ethereum. *Scaling*. https://ethereum.org/en/developers/docs/scaling/. Accessed: 2025-04-01. 2025.

[32] Ethereum. *What is Ethereum? The foundation for our digital future*. https://ethereum.org/en/what-is-ethereum/. Accessed: 2024-06-04. 2024.

[33] Ethereum. *Zero-knowledge rollups*. https://ethereum.org/en/developers/docs/scaling/zk-rollups/. Accessed: 2025-02-16. 2025.

[34] Fireblocks. *What is MPC (Multi-Party Computation)?* https://www.fireblocks.com/what-is-mpc/. Accessed: 2025-01-30. 2025.

[35] Google. *Confidential VM overview*. https://cloud.google.com/confidential-computing/confidential-vm/docs/confidential-vm-overview. Accessed: 2025-04-02. 2025.

[36] Google. *Supporting two phase commit protocol in blockchain system*. https://patents.google.com/patent/US20240346011A1/en. Accessed: 2025-06-04. 2025.

[37] Brazilian Government. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. https://www.gov.br/inss/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais. Accessed: 2024-12-29. 2021.

[38] Daniel de Haro Moraes et al. *Applying Post-Quantum Cryptography Algorithms to a DLT-Based CBDC Infrastructure: Comparative and Feasibility Analysis*. Cryptology ePrint Archive, Paper 2024/1206. 2024. URL: https://eprint.iacr.org/2024/1206.

[39] Khondokar Fida Hasan et al. "A Framework for Migrating to Post-Quantum Cryptography. Security Dependency Analysis and Case Studies". In: *IEEE Access* 12 (2024), pp. 23427–23450. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2024.3360412.

[40] HKMA. *HKMA launches Project Ensemble Sandbox to accelerate adoption of tokenisation*. https://www.hkma.gov.hk/eng/news-and-media/press-releases/2024/08/20240828-3/. Accessed: 2024-09-15. 2024.

[41] Yining Hu et al. "Blockchain-based Smart Contracts - Applications and Challenges". In: *arXiv preprint arXiv:1810.04699* (2018).

[42] Hyperledger Foundation. *Hyperledger Besu*. https://www.hyperledger.org/projects/besu. Accessed: May 24, 2024.

[43] Identity. *Identity*. https://www.identity.com/self-sovereign-identity/. Accessed: 2024-11-11. 2024.

[44] E. Kiktenko et al. "Quantum-secured blockchain". In: *Quantum Science and Technology* 3.3 (2018), p. 8.

[45] Evan R. MacQuarrie et al. "The emerging commercial landscape of quantum computing". In: *Nature Reviews Physics* 2.11 (Oct. 2020), pp. 596–598. ISSN: 2522-5820. DOI: 10.1038/s42254-020-00247-5.

[46] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf. 2008.

[47] United Nations. *Digital Public Infrastructure*. https://www.undp.org/digital/digital-public-infrastructure. Accessed: 2025-06-01. 2025.

[48] NIST. Gaithersburg, MD, Dec. 2016. URL: https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information (visited on 03/17/2024).

[49] NIST. *Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography*. https://csrc.nist.gov/pubs/sp/1800/38/iprd-(1)y. Accessed: 2024-02-25. Jan. 2024.

[50] ISO20022 org. *A single standardisation approach (methodology, process, repository) to be used by all financial standards initiatives*. https://www.iso20022.org/. Accessed: 2025-01-24. 2025.

[51] Anoop Kumar Pandey et al. "Cryptographic Challenges and Security in Post Quantum Cryptography Migration. A Prospective Approach". In: *proceedings [...]* 2023 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA). New York: IEEE, Sept. 2023, pp. 1–8. DOI: 10.1109/PKIA58446.2023.10262706. URL: https://ieeexplore.ieee.org/document/10262706 (visited on 03/29/2024).

[52] Ken Peffers et al. "A Design Science Research Methodology for Information Systems Research". In: *Journal of Management Information Systems* 24.3 (2007). Accessed: 2023-01-02, pp. 45–77. DOI: 10.2753/MIS0742-1222240302.

[53] Google Cloud Platform. *Implement Zero Trust*. https://cloud.google.com/architecture/framework/security/implement-zero-trust. Accessed: 2025-06-05. 2025.

[54] Polygon. *Ethereum scalability with zkEVM performance and security*. https://polygon.technology/polygon-zkevm. Accessed: 2025-05-30. 2025.

[55] Polygon. *Web3, Aggregated*. https://polygon.technology/. Accessed: 2025-05-10. 2025.

[56] Oded Regev. "An Efficient Quantum Factoring Algorithm". In: arXiv:2308.06572 (Aug. 2023). DOI: 10.48550/arXiv.2308.06572. URL: http://arxiv.org/abs/2308.06572 (visited on 03/17/2024).

[57] Gideon Samid. *Pattern Devoid Cryptography*. Cryptology ePrint Archive, Paper 2021/1510. 2021. URL: https://eprint.iacr.org/2021/1510.

[58] Peter W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *SIAM Journal on Computing* 26.5 (Oct. 1997), pp. 1484–1509. ISSN: 0097-5397. DOI: 10.1137/S0097539795293172.

[59] Solana. *Powerful for developers. Fast for everyone*. https://solana.com/pt. Accessed: 2025-05-10. 2025.

[60] CBDC Tracker. *Today's Central Bank Digital Currencies Status*. https://cbdctracker.org/. Accessed: 2025-04-14. 2025.

[61] National Cyber Security Centre of United Kingdom. *Zero trust architecture design principles*. https://www.ncsc.gov.uk/collection/zero-trust-architecture. Accessed: 2025-02-22. 2023.

[62] Henrique Videira. *Listrack: a custom interoperability design for regulated blockchains*. Tech. rep. 2025. DOI: 10.36227/techrxiv.174650571.12702688/v1.

[63] Qiping Wang, Raymond Yiu Keung Lau, and Xudong Mao. "Blockchain-Enabled Smart Contracts for Enhancing Distributor-to-Consumer Transactions". In: *IEEE Consumer Electronics Magazine* 8.6 (2019), pp. 22–28. DOI: 10.1109/MCE.2019.2941346.

[64] World Economic Forum. *Modernizing Financial Markets with WCBDC*. Accessed: 2025-05-22. 2024.

[65] Zeeve. *Exploring the Benefits of Account Abstraction in Rollups*. https://www.zeeve.io/blog/exploring-the-benefits-of-account-abstraction-in-rollups/. Accessed: 2025-03-26. 2023.